HIT Standards Committee
Final Transcript
November 30, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good afternoon, everybody, and welcome to the 19th meeting of the HIT Standards Committee. This is a Federal Advisory Committee, so there will be opportunity at the end of the call for the public to make comments, and a record of the meeting will be on the ONC Web site. Just a reminder to committee members, it's especially important today since this is a virtual meeting for you all to identify yourselves when speaking.

Let me do a quick roll call. Dr. Jonathan Perlin?

Jonathan Perlin – Hospital Corporation of America – CMO & President
Good morning.

Judy Sparrow – Office of the National Coordinator – Executive Director
John Halamka?

John Halamka – Harvard Medical School – Chief Information Officer
Present.

Judy Sparrow – Office of the National Coordinator – Executive Director
Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Anne Castro? Aneesh Chopra? Chris Chute?

Christopher Chute – Mayo Clinic – VC Data Gov. & Health IT Standards
Present.

Judy Sparrow – Office of the National Coordinator – Executive Director
Janet Corrigan? John Derr?

John Derr – Golden Living LLC – Chief Technology Strategic Officer
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Carol Diamond?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Jamie Ferguson is dialing in a little late. Steve Findlay? Linda Fischetti?

Linda Fischetti – VHA – Chief Health Informatics Officer
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Kamie Roberts, are you on for Cita Furlani?

Kamie Roberts – NIST – IT Lab Grant Program Manager
Yes, I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Martin Harris? Stan Huff?

Stan Huff – Intermountain Healthcare – Chief Medical Informatics Officer
Present.

Judy Sparrow – Office of the National Coordinator – Executive Director
David Kates, are you on for Kevin Hutchinson? Liz Johnson?

Elizabeth Johnson – Tenet Healthcare – VP Applied Clinical Informatics
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
John Klimek? I know he's on. David McCallie is joining a little late. Judy Murphy?

Judy Murphy – Aurora Healthcare – Vice President of Applications
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Nancy Orvis? Marc Overhage? Wes Rishel? Cris Ross?

Cris Ross – LabHub – CIO
Present.

Judy Sparrow – Office of the National Coordinator – Executive Director
Rick Stephens? Walter Suarez? He might be a little late joining. Sharon Terry or Natasha Green, are you on? Karen Trudel? Jim Walker?

Jim Walker – Geisinger Health Systems – Chief Health Information Officer
Good morning.

Judy Sparrow – Office of the National Coordinator – Executive Director
Good morning. I believe we have a number of the presenters on. John Feikema, are you on?

John Feikema – VisionShare – President
Yes, I am.

Judy Sparrow – Office of the National Coordinator – Executive Director
Peter Tippett? Joe Carlson?

Joseph Carlson – Covisint – Director, Data Exchange Services
Yes, I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Anand Shroff?

Anand Shroff – Axolotl – Vice President, Products
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Cris Ross, I know you're on. Eric Dishman?

Eric Dishman – Intel Digital Health Group – Director Health Innovation & Policy
Yes, and Garry is here with me as well.

Judy Sparrow – Office of the National Coordinator – Executive Director
Dr. Blumenthal, are you on the line yet?

David Blumenthal – Department of HHS – National Coordinator for Health IT
I am.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. I'll turn it over to you then for some opening remarks

David Blumenthal – Department of HHS – National Coordinator for Health IT
Thank you. Jonathan Perlin, are you there?

Jonathan Perlin – Hospital Corporation of America – CMO & President
Yes. Good morning, David.

David Blumenthal – Department of HHS – National Coordinator for Health IT
Good morning. John Halamka, is he on as well?

John Halamka – Harvard Medical School – Chief Information Officer
I am here.

David Blumenthal – Department of HHS – National Coordinator for Health IT
Good morning, both of you.

John Halamka – Harvard Medical School – Chief Information Officer
Good morning.

David Blumenthal – Department of HHS – National Coordinator for Health IT
We're entering the holiday season and, in the past, we have made sure that our federal advisory committees had no rest during the holiday season. I think things will be a little bit easier this holiday season, but I assure you we'll have plenty of work for you going forward, so we will continue to take advantage of your skills and insights. We, of course, are anxiously waiting to see what happens when stage one of meaningful use goes live. I guess it already has gone live for the hospital community, but when it goes live for the full physician community January 1st, and so our understanding of how our standards are being used, received, practically implemented, will be very important.

Then, as we begin to pursue the discussion about what meaningful use stage two will look like. First at a conceptual level, and then with increasing specificity over the winter and spring, having the standards committee working arm-in-arm with the policy committee to make sure that our policy recommendations are implementable in terms of standards and certification criteria will be really important. Of course, we are continuing, at many levels, to work on specific issues, health information exchange, privacy and security, directories, authentication, a whole range of other things, governance, a whole range of other things that you all are aware of and that will affect the work of this advisory group.

We look forward to continuing to benefit from your help and support, and to have you channel for us at ONC and in the Administration more broadly, concerns, views of members of the standards community, the expertise they bring, as well as the other stakeholders that you are linked to and that are working with us to try to make the HITECH Act a success. I will conclude there and turn it over to Jonathan, thanking him for his service. He'll, I guess, review the agenda.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Thank you, Dr. Blumenthal. Let me just begin by taking note of the point in the year, as we approach the holidays and hope everyone had a good Thanksgiving. It really is quite remarkable. I hope everyone shares a sense of optimism and accomplishment. A lot has been done, and much of that is testament to the work of all who have participated on the various committees, but I especially want to provide thanks to the Office of the National Coordinator, Dr. Blumenthal and team.

While we may have a modest break in some of the speed of action over the holidays, I know that the Office of the National Coordinator continues to really push forward. I hope everyone shares a sense of not only the optimism and excitement, but a sense of what many of us have hoped for, a world that's supported by electronic and interoperable health information is beginning to be realized, and today's meeting is really critical to the continuation of that journey. Many of us have been watching in our own environments and amongst colleagues and associates, the beginning of the personal computer revolution in practice environments, clinical environments. The next revolution is really the linking of that information, the analog of the Internet revolution, and that's really why today's discussion is so important, as we talk about mechanisms for really sharing health information. In fact, the major part of our time together today is to discuss standards for routing health information data and to get your input, particularly as we think about that being so much of the platform on which nationwide exchange of health information really will reside. For that, I want to offer a special thanks to all of the presenters.

Before I turn to John Halamka to offer his usual sage insights on this discussion, I want to make sure that I don't fall on my required task as chair. I trust that everyone has had a chance to look at the minutes of the last meeting. Let me again comment Judy Sparrow and the entire team. Your thoughtful capture of a complex discussion is really masterful, but if there are any comments, recommendations, amendments, I'd ask the members of the committee to please identify so. I'll let you take a second to just check your notes on that, if there's anything you want to offer.

As you review that, I'd also ask for your help. A virtual meeting is in many ways, I believe, far tougher than face-to-face. Your offices, if they're like mine, are prone to potential distraction of individuals walking in, just as someone is at my door right now with Krispy Kreme donuts, which after Thanksgiving, I will avoid studiously, but ask for your full engagement in today's important discussion and, again, a particular thanks to our guest presenters. Any recommendations, amendments on the minutes?

Kamie Roberts – NIST – IT Lab Grant Program Manager
On the top of page three, during the last meeting, I was asked the question, and just immediately after the meeting, I responded and e-mailed everybody. I'd like to have that added to the minutes.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Judy, can that be done?

Judy Sparrow – Office of the National Coordinator – Executive Director
That will be done.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Any other comments? With that, then let's declare consensus on the minutes and move forward, and my pleasure to turn the mic over to John Halamka for an introduction of today's discussions.

John Halamka – Harvard Medical School – Chief Information Officer
Thanks so much, and good morning everybody. Today's discussion is quite important. As Jonathan said, we need to celebrate the fact that we have now a set of content and vocabulary standards that I am seeing significant vendor adoption, hospital implementation, significant rollout that has occurred just over the last six months. However, we have not, in our work today, specified transport standards in a clear and unambiguous way, and we did that purposefully, recognizing this was very much still a work in progress, an evolution. The risk we have is that as ONC has its cooperative use agreements with our various states and regions that we'll end up with 50 different transport mechanisms, all of which are incompatible.

Of course, we have the NHIN Connect, and we have the NHIN Direct, now called the Direct Project, which are attempting some convergence to insure that we have simple, scalable, direct, and secure transport that enables us to get data from point A to point B. A challenge that we will have as a committee is taking an objective look at the Direct Project effort and ask, "Has it met its goals, as I said, simple, direct, scalable, and secure?" As background for that evaluation, hearing from leaders in the industry who have enabled healthcare information exchange from point A to point B is very important. By hearing from the testifiers today—Verizon, VisionShare, Covisint, Axolotl, SureScripts, and Intel—we'll get a sense of what has worked and what has not worked. Where there have been lessons learned? Where is security good enough? Where are there scalability challenges? Where are there issues with standards maturity? What are the gaps in standards?

I think of today's testimony as providing extremely valuable foundation that gets us to that next step of objective evaluation of the merits of the Direct Project on its own. What you hope is that we, as a society, come to convergence of a very simple way or simple ways, a few of them, to get data from point A to point B to fulfill various use cases. To me, transport is that last great gap we have in achieving interoperability in this country and getting to where we're going to need to be for stage two and three and accountable care nirvana.

With that, Jonathan, I turn it back to you, and I guess we're starting with the implementation workgroup testimony.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Thank you, John, very much as always, for your very thoughtful introduction. I've heard Judy Murphy, and I believe Liz Johnson is also on, so let us then go to Liz Johnson and Judy Murphy for a report from the implementation workgroup.

Elizabeth Johnson – Tenet Healthcare – VP Applied Clinical Informatics
We'll be glad to do that. We're going to do this very quickly. As you notice, Judy and I have put together just a few slides keeping in time with the quick amount of time we have on the agenda this time so that we can get to where we're all anxious to hear about transport, so go to the next slide, please. Most of you are familiar with our workgroup team, and thanks to all of these folks. Everyone has been actively engaged in helping us move forward to an activity that we have coming up in January that we want to talk about for just a few minutes this morning.

What we are really working on diligently through November and December is two things, the first thing being putting together our January 2011 hearing entitled *Real World Experiences: Working with meaningful use*. We'll talk about the panels that we intend to establish for that hearing and the questions that will be answered. Then, secondly, we're working with Doug Fridsma and the HIT Policy Committee adoption workgroup to really work together in this arena because we have some areas where we can supplement each other's knowledge and contacts so that we can be sure that the policy and standards committee move forward around meaningful use and our knowledge in a very constructive way.

We've talked about this. There's been a little bit of reorganizing around the panels, but they're very similar to what we've talked to you about in the past. We'll do five panels. The first one will be one around supporting implementation, looking at the role of the regional extension centers and the certifiers. Then we'll look at the early adopters of meaningful use that are beginning to get into the process of seeking attestation during fiscal year 2011 for the government or even moving into 2012. We'll look at two groups from a consistency perspective. First, we'll look at eligible providers, both small and large practices, and then we'll look at our hospitals. Obviously, they fall into three categories: small, large, and IDNs. The idea being is that we want to cover the consistency of the populations that will be getting into the meaningful use attestation arena and gather information from them to be shared with our populations that we serve in terms of the standards committee.

The next thing we want to really look at is meaningful use, and there are a number of opportunities where we can gather information around workforce issues, the actual metrics themselves, the preparedness of

the vendors, and obviously, we'd be covering both performance and quality. Then, finally, we want to look at operationalizing exchange, which is very appropriate for today's discussion. But how are we doing with the HIEs, both at the state level and the private level, in preparing to move into the next sort of generation of actually taking information outside of the four walls of the place where you provide the care and making that information available in a much more wide scale basis?

Then, finally, I want to look at our last slide, which illuminates the kind of questions that we will be presenting to each one of the panelists. Then we'll be, as Judy and I and Judy Sparrow, call and talk with these panelists to prepare them, this is the guidance that we will give them on the kind of testimony that we would like in two formats. Certainly in written format, as we've seen prepared for today's meeting, but also in their comments during the panel session, as well as in response to us who will be conducting the panel. So we're really looking at, based on the reason we asked you to join our panel, what are your challenges, barriers? What are you using for your approaches? What has worked? Where are you struggling so that we might be able to add some assistance in that arena? What have been your outcomes to date? What do you anticipate issues to be in the future? How might you mitigate them? Then we really are looking towards always real life stories so that we can translate conceptual frameworks into real experience.

Again, respecting the time that we've been allocated, that's where we are. I know that Judy and I will be meeting with the workgroup on Thursday to begin to finalize the panelists and when we're back in December to give the committee a full report on the actual representation on each panel and so on. Judy, I would ask you if you'd like to add to that very quick summary.

Judy Murphy – Aurora Healthcare – Vice President of Applications
The only thing that we probably haven't done, I don't think, is give people the dates. We are talking about doing this just prior to the January 12th meeting of the standards committee, looking at the afternoon of Monday the 10th and all day on Tuesday the 11th. Of course, you would all be invited to participate, attend, observe, and be part of the panel asking questions. Any of you who are able to attend, please feel free to make your travel plans accordingly.

The only other thing about the panelist questions that became—obviously as you were reviewing them was we also intend to get feedback from folks in terms of the communication, both around the standards and around the meaningful use measures, and talk a bit about what might have made that more, what worked and what didn't work. So that as we get into stage two, we can make sure that we beef up or shore up that communications in areas that maybe were not ideal in the past.

Elizabeth Johnson – Tenet Healthcare – VP Applied Clinical Informatics
Great point. John, we'll turn it back over to you for any further input. That's the conclusion of our report.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Thank you both, Liz Johnson and Judy Murphy, for your introductions. Why don't we open for any questions or comments from the committee? I'd just ask that because we're virtual that you identify yourself as you speak. John Halamka, any comments that you'd like to offer?

John Halamka – Harvard Medical School – Chief Information Officer
No. I just think it's incredibly important work because, remember that as we move from stage one to stage two and three, CMS and ONC are really desiring feedback as to how successful organizations and eligible professionals are being in actually getting to the adoption of the technology and the standards and its meaningful use. I presume that if we discover that over the course of the six months of 2011 during the reporting period that there actually are real struggles, that that will substantially influence how stage two and three's aggressiveness and pace are rolled out. So just certainly applaud Liz and Judy's effort because hearing from people doing this in the trenches and understanding where they're running into tough points is key for us to, I think, as you said in the past, with the implementation workgroup is where the rubber meets the road. Really, make sure our recommendations from the HIT Standards Committee are reflective of the realities of the marketplace and the people in the trenches implementing.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Well said. Let me, again, thank you both, Liz Johnson and Judy Murphy. Terrific work, and appreciate everyone's engagement in your upcoming meeting and testimony. I believe that Jamie Ferguson is calling in from London. I just want to check if Jamie has joined. We'll leave our world traveler to update later. John Halamka, anything that you'd like to update from the clinical standards workgroup?

John Halamka – Harvard Medical School – Chief Information Officer
Just in general, one of the threads that Jamie would like to pursue is device standards. Now we recognize that as accountable care organizations form, as healthcare reform becomes a reality, there may be more homecare. There may be more distributed use of devices measuring blood pressure or measuring glucometers interfacing to PHRs and EHRs. We better be sure that these various devices that we're going to see becoming more ubiquitous have the right content, vocabulary, and transmission standards.

Specifically, Jamie is interested in looking at content and vocabulary in the immediate term, and I think actually we're going to hear today from Intel on some aspects of transport because Intel has done quite a lot of work on devices. Of course, one would imagine the FDA will be engaged. We'll tackle interesting issues like universal device identifiers, which is something that the industry and the FDA have been talking about for quite a while. I think you can expect that first quarter of 2011 you'll start seeing a number of hearings around device standards. As I recognize, the number of things that the standards committee can do is infinite, but certainly, what I'm seeing is the M-health, whether that means devices in the home or more ubiquitous use of iPads, iPods, etc. is becoming a significant trend, and we should address it.

Jonathan Perlin – Hospital Corporation of America – CMO & President
I applaud that work. I just step to my own experience in the Veterans Health System and Linda Fischetti may want to amplify, but on any given day, there's an average daily census of over 50,000 patients who receive remote physiological monitoring. The ability to really provide support and care outside of the traditional care environment really offers a whole new level of patient freedom and access to clinical support. As well, for those of us who do much of our work in hospitals or clinical offices, it's just kind of ironic that many of the data elements that we use are born digitally, are copied to paper, and in electronic environments reentered. The standards that would allow that continuity of information would really improve not only the accuracy and safety for the obvious reasons, but the timeliness of that information and the quality of the decisions that can be made, so applaud that activity.

John Halamka – Harvard Medical School – Chief Information Officer
Certainly there's ongoing work about getting to that place where we have a repository of vocabulary resources for all meaningful use applications in a simple, downloadable fashion with a rational funding model, so Jamie's group continues to discuss that. The NLM has worked with a number of vendors that's going to have some exciting announcements of some of the progress they've made. I think we are seeing substantial forward movement on all things vocabulary based.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Terrific. I've heard Dixie Baker, I believe, is online. Dixie, anything you'd like to update from the privacy and security workgroup?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I have no update from our group, but given John Halamka's comment from Jamie, I would also like to add that as we hear the testimony today, we should be thinking about transport for devices from the home to the provider entity as well.

Nancy Orvis – U.S. Department of Defense (Health Affairs) – Chief
John, I have one comment if I could make it now or later regarding the standards committee. I think it might be important that we start to clarify the types of medical devices we're talking about standards on. Because not only do we care a great deal about home monitoring or electronic monitoring medical devices, we have to understand that the FDA also publishes metadata and criteria for implantable

devices, and considering that technically medical devices also include everything by two-by-twos and four-by-fours, the whole standards on recording that in the records. The reason I bring that up that we need to look at all three areas of those is because, particularly on our wounded warriors, there may be implanted— We want to be able to track the fact that a patient also has a medical device summary of implanted devices, whether it's a stent or pacemaker with IDs or titanium plates. Or, secondarily for all chronic care patients, there is the category of devices called durable medical equipment. Again, if any of those things are— Durable medical equipment includes artificial limbs, as well as walkers and other kinds of things. While it is very important that we get working on the electronic transport of data for monitoring devices, it is also, I think, very important that we look at creating patient care summaries of their durable medical equipment that they need to function in chronic conditions.

Secondarily, a list of implanted devices with identifier numbers so that they know when or if anything has to be replaced. I just wanted to make that comment. We will be working on the standards committee with that. My military logisticians are very active in the GS1 work area for that very reason, so I just wanted to bring that up that there is more in this category than strictly the electronic monitoring data coming in. Although that is very important, I think we also need to work on putting in the record the durable medical equipment and implantable devices.

Jonathan Perlin – Hospital Corporation of America – CMO & President
I think your point is very well taken. I get the sense that that will be a very robust discussion in terms of identifying not only the different categories, but some priorities in terms of being able to provide some insight and guidance on the interoperability standards. You've essentially identified that you need to have a way to categorize the different devices before you can actually really parse to the interoperability aspects.

I'd just note that this is an area that I think may be broader than this discussion sort of telegraphs when one thinks of other challenges. For example, the FDA has been leading a discussion about the appropriate use of radiation, both diagnostically and therapeutically, and how does one actually provide a consolidation or a consolidated repository of cumulative radiation doses that patients have experienced? This discussion of device and implications of standards around the use of devices and the presence of devices and the experience of patients with devices is very broad and appreciate your identification of the breadth of that and look forward to the work of the standards committee in sort of scoping the field and then identifying some first activities.

John Derr – Golden Living LLC – Chief Technology Strategic Officer
Jonathan, I just wanted to add telemedicine to that and also how important the monitoring devices are to homecare and to nursing homes, as we move forward.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Terrific point.

John Halamka – Harvard Medical School – Chief Information Officer
Right, and just to clarify, in the conversations that I've had with Jamie, it ranged from what if your tennis shoes have pedometers in them and need to transmit such information to the PHR and EHR to the what if you have a pacemaker that has a universal identifier associated with it and metadata that might be used to insure you have good continuity of care. Therefore, the metadata around your implantable device is actually included in the continuity of care documents or it is used from a surveillance perspective or a recall perspective, all the way to you might have a device, which is delivering mission critical telemetry in a hospital setting. I think I had used some early examples of homecare, but it's truly all these domains that would be considered.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Terrific discussion. I very much look forward to that, many thanks to you and Jamie for leading that discussion at the clinical standards group. Janet Corrigan and Floyd Eisenberg, anything that you'd like to update from the clinical quality workgroup? Okay. Hearing none—again, I think one of the risks of the virtualness—we will move then on to the agenda. Before we do so, any comments from any of the other

committee members on the workgroup or committee activity in aggregate before we get to really the focus of today's discussion? Okay.

With that then, John Halamka, if you'd like to introduce our next set of discussions around health information data, routing, and then any comments? I guess we're going to Doug Fridsma for that.

John Halamka – Harvard Medical School – Chief Information Officer
Let me start off and then, Doug and Arien, are you on the line?

Arien Malec – RelayHealth – VP, Product Management
We are, at least I am. I think Doug is as well.

John Halamka – Harvard Medical School – Chief Information Officer
Very good. Yesterday, the Direct Project had a major press release describing some successes in the creation of implementation guides and creation of running code and getting support from the vendor community, so really kind of a milestone day, and so I blogged about it. The National eHealth Collaborative just sent out a mailing about it. You'll find a really nice press release and overview.

What these folks have done, as you recall, is put together hundreds of interested stakeholders to look at how REST, SOAP, SMTP, the various transport options might work or not, and how you could create a point-to-point network that enabled the little guy to get data to any other little guy that was simple, direct, scalable, and secure. In their debate, they have come out with a statement that SMTP and S/MIME and TLS for security is a very good way of getting data from point A to point B. By the way, it implies a number of other problems like how do we deal with directories. How do we deal with certificate management? How do we deal with audit trails? Of course, policies that have to exist as to how all this will be governed.

These themes that the Direct Project has wrestled with have also been wrestled with by a number of vendors. There are examples of state regional health information organizations or health information exchanges that are active today that have wrestled with these issues. Today's important discussion will go through 15 minutes of testimony from each vendor who has a product or service they offer that has tried to deal with point-to-point data exchange, directory services, certificate services, audit trailing, and these sorts of things, followed by 15 minutes of Q&A from the committee and reaction from Arien and Doug, who have been, of course, very, very close to the Direct Project. Then, when we finish, I hope that we can try to synthesize some of the lessons learned that we've heard from these six disparate testifiers to give us a sense of how it informs our evaluation of the Direct Project. How we can get to what I described as a parsimony of mechanisms for transport so we have, not 50 different HIEs, but a network of networks that is interoperable.

Arien or Doug, any introductory comments you'd like to make?

Doug Fridsma – ONC – Acting Director, Office of Standards & Interoperability
Thank you, John. I think that that was a nice introduction. I'm looking forward to today's discussion. I think the thing that's important is that although we're going to be focusing a great deal around NHIN Direct and the kind of point-to-point communication, in fact, the Nationwide Health Information Network is more than just that. It's really defined as the standards, the services, and the policies that allow the Internet to be used to securely exchange information. I think what's nice about the testimony and what I hope will happen in our discussion is to think about how the Direct Project fits into this larger toolkit that we have to help support interoperability.

I think we've got both the notion of exchange, which is making sure that our information can move around, and we also have the notion of interoperability, which is, can we use that information in useful ways for clinical decision support or for adverse event reporting or other kinds of things? I think it will be helpful to sort of see where do we need to really provide optionality and alternatives where it really makes a difference in achieving either exchange or interoperability, and where do we need to really settle in on standardized and consistent ways of doing things to support both exchange and interoperability?

With that, Arien?

Arien Malec – RelayHealth – VP, Product Management
No, just to say I'm really looking forward to the testimony, and we will, I think, both have some further comments after the testimony. But I am very impressed at the degree to which a set of organizations and a set of public and private organizations have sprung up recently to address the needs of transport, and I'm very hopeful that what we're seeing is a business model for information exchange and in support of health outcomes. I'm just very encouraged to continue the conversation to see how we can make sure that those business models for exchange and interoperability are themselves interoperable amongst themselves. I think that will be—I would predict—one of the key discussion points after the testimony, but as I said, I'm just really thrilled to hear the testimony.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Just to amplify what Doug and Arien have said, today we are looking a point-to-point push transactions, and that isn't to say that is everything that the country needs. Of course not. There are the famous emergency department unconscious use cases where one needs to pull data. There are a variety of architectures one might imagine, and we have, in Direct, push, but in NHIN Connect, we have pull. This is part of a spectrum of solutions. It just so happens today we're going to be looking at point-to-point push.

Another thing Doug said that's quite important is we all know that interoperability depends on content with metadata and vocabularies and transport, all three. Today, we'll be—yes—talking a lot about transport, but just building a pipe from place-to-place isn't really sufficient if one wants true interoperability, such things as medication reconciliation and decision support, alerts and reminders. It's the combination of good structured content and transport that will get us to the quality, efficiency, and safety goals we have in the future. But, of course, unless we have transport, we can't get started, so it's a very, very important component.

Peter Tippett, are you on the phone?

Peter Tippett – Verizon Business – Vice President Research & Technology
Yes, I am.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Let us turn it over to you to hear from Verizon.

Peter Tippett – Verizon Business – Vice President Research & Technology
Thank you, guys, for having such a great committee and important topic here. I'm really excited to be here today. I thought I'd just give a relatively quick overview answering the questions that were submitted and then open up for the committee to ask further questions.

As many of you know, Verizon started building a little over a year ago a push-oriented network that we called the Verizon Medical Data Exchange. We announced at HIMSS in March that this exchange was running, and we had eight mostly vendor users. This was content management people, a couple of EMR people, and a lot of dictation transcription companies on the theory that people would like to get from the things that they're already creating in some version of electronic form like dictations and Word documents and so on to the next doctor or next hospital.

We mentioned at the time and announced later that the exchange can support any other document type and doesn't require any kind of structure to the document. Then, a couple of weeks ago, we announced that—and that exchange that we put together and was operating since March is really a machine-to-machine exchange. It allows software or applications to join the exchange and, using a restful protocol, send documents to doctors who have other applications connected to an exchange. It would be a transcription platform could send a document to an EMR. That was the original functionality.

A couple of weeks ago, we announced that we added a portal that would allow humans to join the exchange and that, by January, we intended to have three accounts for 2.3 million doctors, nurses, nurse practitioners, and physician assistants. These are the people who are currently in the directory that Verizon supports for this exchange. We also announced that, as part of that, we are going to be issuing X509 identity credentials for both authentication and signing that could be used for anything that credentials need to be used for in the healthcare space requiring an X509 PKI related credentials for either signing or identity. That they would be completed and that we would have further announcements on that in January, but we expect to have that completed.

The credential part of this would allow people to use these identities. They are standard identities that chain up all the way to the worldwide route certificates and, therefore, are trusted by all platforms that currently use any kind of PKI. Then the exchange under this other model would allow, for example, a doctor to log onto an online interface to receive a document that was sent. For example, if someone had a transcription company sent a Word document to Dr. Smith at Mercy Hospital. Dr. Smith at Mercy Hospital was at Mercy Hospital and that hospital had an EMR. The EMR was connected to the exchange, then the document would make it to the right place, and Dr. Smith would either get an alert or it would wind up in the patient's data set for the doctor to review.

If the doctor didn't have an account at that hospital, or if the hospital didn't have an account with the exchange, we still thought that these networks were only worthwhile if you had some reasonable chance of getting data to anyone. So we announced a couple of weeks ago that we will provide an online access portal that all doctors have rights to use at no cost to them individually and, therefore, the document will land in their account. If they want to get a copy of it, they'll just log in with the universal identity, the medical identity that we gave them, and that will give them access electronically.

The first phase of this allows them to receive documents. The interface is meant to be a bit klugy. The whole point of this is to drive people to use EMRs or HIEs, and to get data to those places. The point of it is not to try and make this a system that people want to use as the primary method of moving documents, but sort of as a backup, and encourage people to do more integration of either EMRs or HIEs so that the message is moved the way they ought to.

Your questions ask about authenticating endpoints. On the machine-to-machine side, the program, we do a certification of each endpoint with a series of tests, application and vulnerability testing, a series of questionnaires, things that are all a part of the HIPAA related application and security testing. We also make sure that the application does indeed belong to Mercy Hospital or whomever by physically checking that and being there. Then we issue the hospital and the application a unique SSL certificate and a toolkit. That toolkit and certificate allows that software to join the exchange. It can't do so without a certificate, and it's a two-way handshake between that, that is to say, there's a GLS SSL certificate on both ends of the transaction: on our end, in the middle of this exchange, and on each endpoint. Each endpoint has a HIPAA BAA agreement that allows for the data to get going where it needs to go.

The protocols involved are restful protocols now. They're over HTTP. There is, obviously, an SSL tunnel operating at all times, and the tunnel couldn't connect unless we knew the identity of the machines or software that we're connecting. By January, we will also support the IDE XDR protocol for pushing documents and all the related header things to anybody else that needs it. The SDKs that we're providing to the people that want to hook their equipment and software to this exchange include Java, .NET, and Ruby on Rails. As I mentioned, the identity for people who come to the provider portal, that identity is strong, level three credentials that we have issued to or will have issued to virtually all doctors and nurse practitioners and physician assistants in the country, and that'll be used for them to fill out individually to the portal.

You asked questions about confirming receipt of the message. All messages are hashed. All hashes are signed for all messages traversing this exchange. The machine-to-machine protocols allow for the logs in the middle know when the machine retrieved the message or whether the doctor retrieved the message, and they know whether it was a machine, that is an EMR on behalf of Dr. Smith, or whether it was Dr.

Smith himself. That logging is in there. If Dr. Smith logs in later, and his hospital machine accepted the message, the doctor can learn that the machine got it, but that he didn't, and that granularity is there.

I think that's the basic questions that you asked. A couple of comments that seem to be floating around are is SMTP good enough with S/MIME. The other practice I run at Verizon is a security practice. It's a derivative of ICSA labs and the cyber trust security practice. We do a huge amount of risk related research, including the data breach investigation reports, which the most recent one was the last 930 cases of combined Secret Service and Verizon investigation of worst cases of computer crime, including lots and lots of computer crime against the healthcare system.

I can tell you that a combination of S/MIME and SMTP would have resisted all attacks. That is to say, there were no attacks in the history of the last seven years we've been doing detailed analysis of both our data, which is many thousands of cases, and Secret Service and other law enforcement cases that we have not published yet, and among a couple of thousand companies that use our services, our security services. SMTP and S/MIME combined would resist attacks that are known to exist and ones that are anticipated quite well.

Another question relates to whether or not the content needs to be individually encrypted if it's running inside of an encrypted tunnel like SSL. Our answer to that would be as long as you know who the endpoint is at both ends of the SSL that additional encryption is irrelevant. It doesn't add any value at all. It doesn't reduce any risk at all. By the time the document gets where it's going on the doctor's machine, it's going to be unencrypted either way, and at every point in between it's going to be encrypted either way. As long as you can assure the identity of the doctor by the time it becomes clear text, it's hard to imagine why two layers of encryption offers anything better than one layer of encryption.

With that, I think I'll take a breath and take any questions that you might have. I know I kind of zipped along there, but I thought I'd rather answer your questions than kind of blow our own horn here.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Why don't I start with a question? Arien, I need your help with this one. One of the challenges in thinking about point-to-point communication is how to structure the directory. Do you want a yellow pages that describes the organizational endpoints, or do you want a white pages that describes an individual person-to-person transaction? What certificates do you issue, organizational level or personal level?

I think for a moment about e-mail. Now if I want to look up John Perlin's e-mail address, I actually have no way to do that. I actually have to, by prearrangement, know his e-mail address, but once I know it, there is infrastructure on the Internet to route my message from a gateway at Beth Israel Deaconess to a gateway at HCA. From a Verizon standpoint, as you think about the directory services you're offering, are they yellow pages? Are they white pages? Are certificates at the organizational level or the personal level?

Peter Tippett – Verizon Business – Vice President Research & Technology
They're both, and they're both. The fundamental directory that we have is based on individuals, but it has entries for institutions, so both exist, but each individual has as many personas as is necessary, so Dr. Smith is Dr. Smith as an individual with a persona as a doctor. Dr. Smith's persona as a doctor also includes a persona as a doctor at Mercy Hospital and a doctor at the VA and a doctor at some other place. If the doctor has five different places that the doctor performs services, and all of them are enabled, then the doctor will have five personas, one representing each.

We've organized it so that the queries can figure that out. If you want to send something to somebody by a doctor name at an institution, the first time you ask if that's ever happened before, then it'll already be in the directory, and we'll just route it directly. Each time each institution joins, they declare all the doctors or providers that they believe they represent, then that goes into these persona fields on the directory that we manage. The same is true for each HIE or transcription company or whatever, anything that might be an endpoint or source to the exchange.

In terms of digital certificates, each person gets an identity. It's a set of X509 credentials, both for signing and for authentication. For machines and hospitals, the identity we're giving them right now is an identity that's based on SSL instead of an identity that's based on anything else, so they are given a certificate, and that is their mechanism of joining. We expect that that will have to get a little more complex, but we think that the directory can handle any mixture by making sure that it has the notion of personas and that a hospital could have an entry just like a doctor could.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Arien, reaction to that because I know you've had a lot of thinking about addressing in the Direct Project?

Arien Malec – RelayHealth – VP, Product Management
Actually, the question I'm going to ask is related to Peter's point about TLS being sufficient if you know both endpoints. This actually is related to addressing, if you want a mechanism that has addressing that's universal in nature, and by universal, I'd mean you don't know beforehand who is running the network that serves a particular address. Our observation in the Direct Project was that it was difficult to use TLS unless you had some well-known set of route credentials that everybody could subscribe to. In eCommerce for example, there's a well-known set of route credentials. There's a browser bundle that everyone gets with route certificates that you can assume everybody running an eCommerce sight has, routes up in their certificate. When we looked at the challenge of higher security environments, we couldn't figure out a universal set of route service that we could point to, to make TLS just work in the same sense that it works in eCommerce. What we did was go to content based security using S/MIME and a mechanism that's actually pretty well published for how to discover mutual trust in a security negotiation sense during the content transfer.

I'm wondering if you have any insights into that process and what you think about it. It's related to addressing in a sense that, again, if I have an address—and, John, as you articulated very well—the actual connection is organization-to-organization. Because of the way that the Web works, I don't know whose machine it is beforehand. Before I send that transaction, I only know it after and … bound through the DNS, as I'm figuring out that transaction. Trust and addressing end up being very closely coupled. Peter, I'm just wondering what your reaction is to that overall problem statement.

Peter Tippett – Verizon Business – Vice President Research & Technology
I think you're obviously worried about the right things. I don't see any particular reason why the route certificates that are trusted for commerce can't be exactly the same ones that are trusted for medical information transfer. They're used for nuclear launch codes and all kinds of military secrets and things. Have they been used in the system, the super Net, we wouldn't have had— Well, I guess if people are— I'll skip that part, but these are already distributed. They're already trusted by virtually all of governments and all kinds of technology companies, and they're already deployed in essentially all technologies, including all browsers and all operating systems and all routers and all set top TV boxes and so on, all telephones, all mobile phones that can support anything like encryption already have this stuff deployed. I'd be hard pressed to imagine why we'd want to invent a different route system than the one we've got that works.

But I agree with you that these things aren't inherently findable before the connection is made. The way we get around that on the use of our exchange is that we certify each endpoint before it gets an endpoint certificate. In a sense, it's got certificates on both ends. They are pre-known before they join when it comes to machines. That's a very, very rapid process and very inexpensive in terms of people time. It just takes a bit long to install a certificate, so it shouldn't be terribly onerous to do that. But that's how we tried to solve the same problem.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Let us open it up to others on the committee who have questions.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Peter, I may have missed it in your summary because you covered a lot of ground, but my simple question is, will your network be address compatible with the Direct network, with those who are using

Direct? As you know, one of our goals in Direct was to create universal addressing so that a provider who has the secure address of his intended recipient would not have to worry which vendor or which HIE or which nationwide provider of the mailbox was actually providing that mailbox, but would be assured that the message got there in a secure fashion. That requires interoperability across the system, which either means that everyone implements the same protocol or that appropriate gateways are in place to bridge between disparate protocols. My question is will your network be interoperable with Direct? If so, how will you achieve that? Thanks.

Peter Tippett – Verizon Business – Vice President Research & Technology
Yes, thanks. It is not right now, but our plan is for it to be interoperable with Direct, both through the XDR interfaces, and we expect this. I guess I didn't mention, Verizon also has a traditional HIE, an NHIN Connect oriented system with structured data and all the various protocols for both push and pull there. We expect that this exchange will, it isn't right now, but we expect within a month and a half or two, it will be connected to the rest of the NHIN Connect related system and, therefore, from there, to anywhere else. Yes, right now no, it is not Direct compliant, but we expect that it will be, but through several protocols.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you, Peter. I appreciate your testimony. Like Arien, I had a question about your statement about the content not needing to be encrypted as long as the two ends of the FSL tunnel are known to each other. I agree. But my question has to do with, when you issue your machine certificates, do you care whether those machines are EHR servers versus Web servers or whatever because obviously if it's a Web server, then when it hits the endpoint, it gets decrypted and then folded and encrypted within the organization. I was wondering about what you certify, whether you certify the endpoints as EHR machines or Web servers or any other kind of machines.

Peter Tippett – Verizon Business – Vice President Research & Technology
Yes. The endpoints so far and the only ones we anticipate are EHR like machines. They might not be called EHRs by the institution. They might be called a document management system, or they might be called something like that because they might not be as compliant as an EHR would be, but they have the same function. They take data about patients and store it in some way with doctor affiliations or have a mailbox for doctors or some kind of a messaging system for doctors. That's the kind of endpoints that we are hooking this thing to when it's a machine-to-machine thing. Therefore, that system—and those machines are being certified by ICSA labs, and other labs are welcome to do the— We don't care whether it's ICSA or somebody else, but we're requiring that they get a level of certification to make sure they're resistant to attack and that they have basic security turned on, including account control and so on. That's the mechanism of controlling the problem that you describe.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Then that leads to, you also mentioned that the certification of the endpoints is relatively easy and quick.

Peter Tippett – Verizon Business – Vice President Research & Technology
It can be if it's an already reasonably well put together system. For anything that's broken, then it's not. Then the testing is easy, but the fixing might not be quick.

Jonathan Perlin – Hospital Corporation of America – CMO & President
One of the things, Peter, I'm wondering is, as we do our evaluation of Direct and its implementation guides, is there an implementation guide Verizon has available for software vendors to incorporate your HIE functionality in their products so that we might use just as a basis of comparison?

Peter Tippett – Verizon Business – Vice President Research & Technology
Yes. We've got an SDK toolkit, some training guides, people that have the training capability. All of that stuff has been in various crude forms over the last nine months. We can figure out which parts of it would be the most useful to share with your committee. Sure.

Jonathan Perlin – Hospital Corporation of America – CMO & President

I would defer that to Dixie because, Dixie, your group will be leading this evaluation. I'm just thinking that especially on some of these trickier problems we've heard about, certificate management and establishing trust relationships, looking at their implementation guide might be helpful.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I agree. Thank you.

Peter Tippett – Verizon Business – Vice President Research & Technology
You bet.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Any other questions?

Arien Malec – RelayHealth – VP, Product Management
John, I just have one follow up question for Peter. Actually, my issue about the typical browser bundle actually related to identity management and the level of identity management that the typical certificate issuers for eCommerce provide to the purchasers of their certificates. I guess the follow up question is, do you believe that the processes that those organizations use to supply eCommerce certs are sufficient for identity assurance at a level that's … with healthcare?

Peter Tippett – Verizon Business – Vice President Research & Technology
No, I think I agree with you there, but what I was sort of going to was that route certs are well done by everybody who has route certs. They're tested by numerous organizations annually. It's a very rigorous system, and I think the route system is well run, and there isn't any real need to invent a new one or use new route systems.

Yes, SSL certs you can get for going online, click, click, click, and your fax winds up in some hard disk storage somewhere, and no one ever looks at it, no one ever reviews it, and you get a server side certificate. It isn't the way we do them, but it's true that there are lots of those happening in the world. That's the reason why we're insisting on either the certificates that we issue or an equivalent system for systems that are on the endpoints of the exchange that we're providing. The equivalent system would be close to the extended, what's it called, extended something certificates, the newer. The only thing we're adding to that is machine penetration and vulnerability testing and physical visit by someone to assure it's the right place.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Any final questions?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Peter, you referred to the signing certificates that you were going to make available, I believe you said, for free. My question is, for someone who is using a different provider of the mailbox service, would they be able to use those signing certificates through an API, through—I believe I've heard on some other conversations about this that you plan to support some standard protocols like Kerberos and OAF. How would those services be provided to third parties?

Peter Tippett – Verizon Business – Vice President Research & Technology
We're right now not providing. We're going to provide all the details about how this massive deployment of identities to healthcare providers works in January, but I will say today that these are standard X509 credentials. They work just like any other standard X509 credential. If you ask them to encrypt something, they will. If you ask the system to do work, it operates exactly as you would expect. Credentials operate if it's being carried around in the hands of a doctor on a smart card or a token or however they want to do it. It will operate with anything that can deal with X509, which is any PKI system that we choose to use, so it should work fine for any other NHIN Direct or any other e-prescribing system that anybody wants to use.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Has there been a charge for the validation service if you wanted to use it, for example, for authentication?

Peter Tippett – Verizon Business – Vice President Research & Technology
As I mentioned, the details of how this is going to actually work are things we're going to hold off until January until we get a much larger deployment than what we have now. We do have a huge operation underway making this thing work, but let me just reassure you that it will work, and it will be, let's just say, significantly cheaper than doing it any other way. How about that?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Thanks. I'll look forward to January.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Thanks so much, Peter, for all of your remarks. I'm sure you'll be hearing from us again, as we go through our evaluation phase.

Peter Tippett – Verizon Business – Vice President Research & Technology
You bet. I'll stick around and listen. That's the plan.

Jonathan Perlin – Hospital Corporation of America – CMO & President
That's just fine. Now let us turn to VisionShare and John Feikema. I, of course, know you're often sitting in the back of our HIT Standards Committee, so you know some of the issues we have been wrestling with and very happy to hear your remarks.

John Feikema – VisionShare – President
Thanks very much for the privilege of providing testimony to the standards committee and guests this morning. We're honored to be able to submit our thoughts and experiences. I have listened repeatedly to the issues that have gone back and forth across the tables there and am pleased to be able to offer a few thoughts regarding standards and approaches for secure, point-to-point transport. We've very supportive of and pleased with the work of the Office of the National Coordinator to help drive widespread adoption and meaningful use of health records and, in particular, the Direct Project has been a notable step forward in this direction, and we're pleased to be a small part of it.

The VisionShare approach to building successful healthcare communications has been founded from the onset with really four key principles. One is we want to be able to utilize the ubiquity and affordability of the Internet to enable participations by big and small players. From our beginning, we built public key infrastructure security into every facet of our communication to make sure that data is private, authenticated, demonstrates integrity and non-repudiation. We've built bulletproof, scalable business practices and tools around user identity verification, a process that requires, for example, a presentation of a government issued ID before we issue a certificate. We increased network participation and adoption by providing a wide variety of onramps and by making technological complexity transparent to the end user. I'll share some of these.

Based on those principles, and with several user refinement, we built an Internet based, PKI secured, healthcare data network that today is utilized by over 3,000 hospitals and a total of about 16,000 different addresses. Large hospitals typically use VisionShare server appliances as their secure gateway to trading partners where distributed entities or small clinics often just choose an X509 client certificate Web portal as a simple way to participate. We've also spent some time working with practice management and EMR vendors; enabling them to choose an X509 client certificate authenticated REST based secure API so that they can build into their workflow access to the data behind the scenes. REST stands for, as I'm sure many know, representational state transfer, and is a lightweight approach to programmatically interfacing with the VisionShare network. But in order to be compliant with our PKI principles, we make sure that each endpoint on that REST API uses an X509 client certificate authenticated TLP session.

All communication within our network requires the use of these certificates, and a server certificate and associated private keys, regardless of whether the client environment is a Web browser, a VisionShare

appliance, or an SCAPI enabled medical record system. In all cases, the TLS handshake protocol is used to provide client and server authentication. Once the handshake is complete, the VisionShare server software can utilize unique names within the X509 client cert to authorize access to specific services and write log entries. Persistent messages are PKI signed using the underlying SHA 256 hash and PKI encrypted using an AES symmetric encryption algorithm.

The VisionShare network is secured by X509 certificates and private keys that are issued by a tightly controlled, VisionShare certificate authority that we call Neutralus. Without exception, every end user of an X509 certificate and private key has completed a stringent identity verification process, which includes the presentation of a valid, government issued, picture ID. Through years of careful refinement, we've also created a scalable and secure certificate generation and distribution process. If a user is diligent in completing his portion of the process, he or she can be up and running on the VisionShare network in a matter of hours. Supporting the business process is a set of infrastructure tools that we use to enable the efficient management of those trading partner IDs, trading partner users, and network monitoring.

Each certificate contains a unique user identifier in the subject-distinguished name that servers as the user's address on the VisionShare network. Nodes on the VisionShare network maintain a distributed map of routing information that is used after appropriate authentication and authorization to send data directly to the recipient node. When we talked about Direct integration in a second, that will be important.

We also think it's extremely important to reduce the complexity for users. To do that, we've enabled this REST based API to provide a simple and practical secure onramp for healthcare messaging. While RESET may not inherently provide message level security mechanisms to insure privacy integrity non-repudiation, our approach combines REST with PKI signatures and encryption of persistent messages, thereby addressing this concern. The combination gives the healthcare entity the option of a much simpler interface into the healthcare message exchange network while maintaining message integrity, privacy, and non-repudiation.

We built an understanding of how much complexity through the years each segment of the healthcare market can handle. Obviously institutional players, hospitals are generally more sophisticated, while when you talk to a small clinic about a data center, at best, it's a closet. It's typically just whatever computer the front desk is running on. We've built systems that can securely tailor the interface for various types of users, allowing quicker adoption of new innovations through protocol bridging.

The architecture and implementation of our network is strikingly similar to the Direct Project. From a provider point of view, a VisionShare server, hosted or locally installed, plays the role of a HISP, the health information service provider, in the context of the VisionShare network. In other words, it handles PKI security, presents a wide variety of secure edge protocols, routes messages, and simplifies the experience of secure data exchange. In a nutshell, it meets the provider where he's at today and enables rational evolution to the exchange needs of tomorrow.

In order to achieve end-to-end privacy, authentication, integrity, and non-repudiation, the Direct Project specifies payload signing and encryption through X509 certs, combined with the S/MIME standard. The VisionShare platform also implies X509 certs for both payload PKI operations and TLS based machine-to-machine authentication and authorization. The S/MIME standard has also been employed within our product line for years. When a message arrives at its destination within the network, the principles of PKI, signatures and encryption, insure that it came from the advertised party and could not have been seen by anyone other than the intended receiver.

For us, the Direct Project has served as an excellent venue for the discussion and trial of techniques and policies surrounding the management and distribution of private keys and X509 certificates. The VisionShare Direct HISP has successfully interoperated with other HISPs using production DNS as a readily available, scalable, and proven certificate directory. The VisionShare network is primarily used in Neutralus, as I mentioned earlier, but in certain controlled situations, much I'm sure like the situations that Peter described, certificates issued from third party certificate authorities have been allowed on the edge of the network, but only after the policies and procedures of the third party CA were scrutinized and

evaluated. The Direct Project allows a more diverse CA environment, which we believe will foster innovation and improve secure communication if done within a clear set of policy guidelines. As mentioned earlier, property identity verification is a critical link in the chain of trust that VisionShare has created and that the Direct Project will create over time.

The required Direct Project backbone protocol, in other words HISP-to-HISP communications, is SMTP. The VisionShare network has mostly utilized client certificate authenticated HTTPS as our backbone protocol. In the context of a payload based security infrastructure such as S/MIME, the specific protocol used on the backbone lessens in importance. What the Direct Project has done correctly, we believe, is choose a ubiquitous and well-known backbone protocol in SMTP, thereby lowering the barrier to HISP participation. This, we believe, was clearly demonstrated at the Direct Project Connect-a-thon in San Francisco last month.

One other interesting component of the Direct Project is the notion of edge protocols. It's the communication mechanism used by providers to communicate with their HISP. In Direct today, this is typically represented as an e-mail client speaking SMTP, POP, IMAP, over TLS to its HISP. Much of the flexibility and ease of use that is inherent in our network emanates from the wide variety of secure edge protocols and deployment options that providers can use to speak to their VisionShare server. It's the existence of the edge protocol concept in both our network and the Direct Project that allows providers to securely communicate today using protocols that leverage existing investments of time and money.

For example, in our network, a provider may use SMTP to communicate with their resident VisionShare server. The server signs, PKI signs, encrypts the data using the backbone protocol HTTPS, routes the message to the destination server. The destination server PKI decrypts, verifies the message, delivers it to the receiver using a secure edge protocol that they're comfortable with, which could be completely different than the sender. The Direct Project architecture is conceptually identical with small variations in protocol choices. The end result is a provider-to-provider secure communication that meets each provider where it is at technologically while simultaneously insulating each side from the protocol details of the other, and we think that's absolutely critical.

The VisionShare Direct public health pilot initiatives are meeting public health departments where they're at today by using CNMS as an edge protocol. The provider side of the communication can choose from any of other VisionShare's other 20 different onramps that we built or other Direct supported edge protocols, and communicate to a public health department who is using CNSM. Both sides now have the freedom to evolve their communications architecture internally without affecting their trading partners.

The Direct Project specifies the message disposition notification e-mail message as a mechanism for sending confirmation of receipt. It will be interesting to see how fully this will be adopted. Our network treats receipts as an application level function and does not have built in receipt confirmation. We haven't heard the request much from our end users, but it will be interesting to see, as we participate more in Direct. It will be interesting to see how that's adopted. Many existing workflows use application level receipts. For example, the X12 network uses a 997 functional acknowledgement. We're excited to see the Direct Project and its match with our network that allows us to enable access to all of VisionShare's existing end users in a Direct compliant way, which we think could give it a nice shot in the arm.

With respect to CONNECT, we first started working with CONNECT when version 2.0 was released in the spring of '09. We've also modeled CONNECT as an edge protocol on our network and have run some experiments to understand its capabilities. Currently we're engaged in deploying a CONNECT gateway as part of the CMS esMD initiative, electronic submission of medical documentation. Our customers will use their existing network capability that we've installed to securely transmit medical documentation to our CONNECT gateway, which will then relay the information on to the CMS gateway. The CONNECT oriented link into CMS is modeled just as an edge protocol on the network, so another destination. We see integrating Direct, the Direct Project in a very similar manner and, in fact, we may be using Direct as a provider protocol to submit information to a CONNECT endpoint at CMS, which would be an interesting twist.

Finally, after ten years of experience moving healthcare data in a PKI secured network, we're pleased with our accomplishments. We believe that we've proven that PKI processes in technology can be deployed on a wide scale successfully. We've proven that the high level architecture on which we've built our network is secure, reliable, and meets the needs of providers where they are today. From an acceptance standpoint, we're pleased that 94% of our customers renew year-to-year with much of that 6% loss coming from typical churn, expected mergers and acquisitions in the provider space. Our customers are insulated from their trading partners, technological choices, and value that insulation much like we believe users of the Direct Project in the future will value that insulation.

There are areas where we believe challenges remain. We know that the semantic interoperability is a challenge for our customers, while it's a giant leap forward to providing the secure communications fabric that providers insulation. There's a same leap needs to occur at the payload level. We're pleased with a lot of the work that's been done on this committee around that already. I believe that that will certainly help. We also recognize that opening up of addressing and routing and security mechanisms will be crucial in allowing networks to expand even more rapidly, and we believe the Direct Project has made a very, very significant leap forward in allowing that to happen.

One of the questions was for some feedback about what we believe looking forward are things that we've learned through this experience. First, we'd recommend that there's no need to ever compromise on insuring privacy, authentication, message integrity, and message non-repudiation within the communications fabric. Placing PKI technology and its processes at the center of one's efforts and maintaining consistent policy and processes for identity verification is important, and we need to clearly state and enforce requirements for securing data at rest.

Second, we believe that creating standards for directed exchange around endpoint addressability, security, and message routing are important, and the Direct Project is an important part of that. We think it's extremely important to enable simple, but secure onramps that hide complexity from the provider without sacrificing security. We think that it's important to allow tools in place, which will meet providers where they are today without forcing them to scrap legacy investments that they've made. And, where possible, we think that it's important to help solve the problem of semantic interoperability. We wholeheartedly believe that the Direct Project has gone a long way toward meeting these requirements, and we're excited to continue our support for that project. Thank you very much for an opportunity to share some of this, this morning.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Thanks very much, John. Why don't I start off with the same question that I asked Peter from a directory standpoint, and in an addressing standpoint? It sounds to me like you are issuing a cert to the combination of person plus organization, and so, in a sense, the VisionShare network is routing from person sender to person recipient. Is that true?

John Feikema – VisionShare – President
I think I'd probably give the same answer that Peter did. Yes and yes. In smaller organizations, it is often a person who is sitting behind the keyboard. In that case, we authenticate down at the end user level. For something, for example, like the Direct pilot that we're embarking on, it would be the destination, for example, would be immunizations@mdh.gov. It would be a departmental level. We always have a specific user attest to the organization and their role within the organization, but not in all cases is the message person-to-person.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Got it. Recognizing that when I ask the question, yellow pages, white pages, or both, I think your answer is both depending on the use case.

John Feikema – VisionShare – President
Exactly.

Jonathan Perlin – Hospital Corporation of America – CMO & President
\ Let me open it up. Arien, any initial comments or thoughts, same issues of certificate management and trust, anything that comes to mind?

Arien Malec – RelayHealth – VP, Product Management
Just an observation that we started the conversation talking about transport, and we've, in both of these conversations, ended really talking about directory identity assurance and trust, and also had the notion of different transport options at the edge, but where trust and identity assurance in the middle is a critical component. I think that's an interesting, common set of experiences between the two first presenters.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Right. I think your observation is key. That is, if there's trust and there's addressing, that the transport standards one uses in the middle, whether those are SMTP, S/MIME, REST, or SOAP, you might have onramps; you might have gateways. The hard part is figuring out who to trust and how to get it there.

John Feikema – VisionShare – President
Yes, I agree. I think that, especially since the technologies can bridge to one another, which means that you can achieve compatibility between them.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Other questions from members of the committee?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Wes Rishel.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Wes, we were so lonely without you.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I know. There was probably hardly anyone there to ask questions, right?

Jonathan Perlin – Hospital Corporation of America – CMO & President
No, we had people standing in for you, so no worries.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'm glad because usually it's the same old hand. Thanks for this presentation. I wanted to add a little strength to your comment at the end about semantic interoperability. Frankly, I think we are embarked on a path of incrementalism, which I strongly favor, getting the connection and getting data there somehow is better than not. As we begin to roll out on a national level, the issues of semantic interoperability will become increasingly important, and as EHRs roll out as well. I just want to emphasize that it's important not to strangle ourselves with hyper semantic interoperability. That is, to find a way to introduce it so that different users in different systems that are at different stages in their lifecycle can continue to interoperate. It's a soapbox I get on every time I get a chance, so I won't go into detail, but I think, as we look forward with all of the work we're doing, we need to recognize that NHIN Direct presents different use cases for semantic interoperability than say NHIN Connect does.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Right. Very well said, Wes. I had mentioned in the introduction to today that there's pull; there's push. There's the notion of quite sophisticated transaction orchestration. Today we're focusing on a simple package, point A to point B, and recognizing that there is value in structure of that content and vocabulary, but that certainly there are many use cases that are simply empowered by just getting the transport, the routing, and the security right.

Other comments that people would make? People are getting shy here. John, all I can say is you must have dazzled them. That's all.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
John, thank you for your presentation and for the contributions that your team has made to the Direct Project. Coming back to my sort of standard soapbox question about universal addressability, I just want to confirm that I heard you say that users on your network would have universal addressability with other Direct Connect users. I believe you implied through a gateway, but I wanted you to clarify that if you could, thank you.

John Feikema – VisionShare – President
Yes. We will have, they will have availability with edge as— We've already integrated the Direct protocol as an edge protocol on our network, so we're able to bridge inbound Direct messages to any one of our endpoints.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So that essentially that is the gateway then.

John Feikema – VisionShare – President
It is the HISP, essentially, yes, and we use VisionShare now as an edge protocol to Direct rather than Direct as an edge protocol to VisionShare, so it depends on which side of the exchange you're on, obviously, but we mapped a way to bridge between those two using a standard Direct e-mail address.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's good. The way that Direct proposes to handle certificates through the certificate discovery mechanisms that have been experimented with, are you comfortable with those? Do you have issues that we should worry about, as we enter into the pilot phase?

John Feikema – VisionShare – President
Well, I think the biggest issue from our perspective is going to be the policies under which those certificates are issued. I think that the technology mechanisms are going to be fine. I think it's as John Halamka said a couple minutes ago. It's about the trust fabric, and we're active in participating on your subcommittee, David, around best practices to try to get at what those issues are.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, and we certainly appreciate all of your input, and thanks.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Dixie, did you have a comment?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I did, but I no longer do. Thank you.

Jonathan Perlin – Hospital Corporation of America – CMO & President
I thought I heard your voice. Any other final comments for John?

Doug Fridsma – ONC – Acting Director, Office of Standards & Interoperability
Just a couple of questions just to clarify: I just want to understand, so when distributing the certificates, are you using the DNS to do that? That was one of the things, I think, discussed in the NHIN Direct Project was figuring out a way to distribute certificates through DNS.

John Feikema – VisionShare – President
For any of our users who implement Direct directly, yes. For those cases where VisionShare is the edge protocol, we have our own mechanism for distributing the certificates. They're created offline. They're sent to the end user out of band. They're sent another key to unlock them, and then they install them in their browser or are installed in their server appliance in their data center.

Doug Fridsma – ONC – Acting Director, Office of Standards & Interoperability

Have you had any experience with say certificate revocation or having to restrict or withdraw certificates that have been issued?

John Feikema – VisionShare – President
We have the ability today, yes, for every end user on our network, to be able to remove their ability to communicate on the network by suspending or revoking. It depends on the specific issue. For a customer that has just asked that their service be suspended temporarily, for example, we put those certs into a suspended mode. For someone that is no longer on the network or has distributed bad behavior, we actually revoke it. We have a CRL today are most likely looking at OCSP.

Doug Fridsma – ONC – Acting Director, Office of Standards & Interoperability
I guess the last question is as we think about different use cases, and we think about kind of directed exchange, or we think about hub/sub or query models, sometimes we can use the certificates to say this person is able to do this kind of communication. They're able to respond to queries, but they're not able to send directed communications, or they can send directed communications but not the other. Do you have any of that kind of differentiation with your certificates?

John Feikema – VisionShare – President
We use the certs a lot in terms of what— What's the right way to say this? The certificate identifies very clearly to us who that end user is. Some of the backend systems that we've developed have married that person to the services that they have, in this case, purchased from us that they use on a regular basis. That is quite extensible to be able to do basically a lookup to say, okay, that end user has the following five services enabled. I'm not sure how much of that we really want to build into the cert itself. It's more of a mapping of the cert to the end user services. Does that make sense?

Doug Fridsma – ONC – Acting Director, Office of Standards & Interoperability
No, that does make sense. I appreciate that. I guess the last question is, you've briefly talked about identity verification and said that you can do this in a matter of hours. Does that include just identity verification? I know that the previous testimony talked a bit about in terms of doing certification against HIPAA standards and things like that. Now obviously we're talking about a slightly different—one is certification. The other is sort of identity verification.

John Feikema – VisionShare – President
Yes.

Doug Fridsma – ONC – Acting Director, Office of Standards & Interoperability
But do you do anything above and beyond just making sure that Dr. Jones is Dr. Jones?

John Feikema – VisionShare – President
When an end user requests to join the network or purchases a service, for example, a single doc shop who signs up to be able to communicate with Medicare for $50 a month or whatever it is, when they sign up, they're presented with a BAA that they sign and fax back to us and sent back to us. They're also presented online with a template that describes what we know about them already. We've been in a conversation, a sales conversation for example, so we know who the end user is, who the technical contact is, for example, and all that is presented to them in a Web page. They're allowed to edit it if we have anything wrong. They then print it out, have it notarized, which is where they present their ID, and then they send it back to us, fax it back to us, and send it hard copy.

From that point, once it arrives, we hit the go button, and everything is live. Everything has already been enabled by the virtue of them having filled that out and printed it. That does the BAA. It does the identity verification process. In the background, we've then turned on the services awaiting the successful completion of that certificate delivery process.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
John, did I understand that you verify the credential by fax?

John Feikema – VisionShare – President
They're allowed to send the fax to us to speed the initial part of the process. We require a physical hard copy.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Is there a human being who looks at the picture ID and looks at the person?

John Feikema – VisionShare – President
In order for them to get it notarized, the notary looks at the ID and looks at the person and verifies.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So it's a public notary that provides that step.

John Feikema – VisionShare – President
Correct, because lying to or misleading a notary is a federal offense.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. Then can you tell us a little bit about the kinds of use cases your network is, again, used for?

John Feikema – VisionShare – President
The predominance today is administrative transactions, and a lot of them for Medicare were the— I think that's one of the trading partners that we've enjoyed the longest. We have a number of other trading partners in the administrative transaction space that are conducting business today. With the Minnesota Department of Health, we also route a lot of HL-7 traffic for immunizations, newborn screening for disease reporting as well.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you for your presentation. You mentioned that in many cases that primarily the end users are persons, but in many cases, they may be departments. Then, in response to Wes' question, you said the primary transactions today are administrative, so I'm curious. I think I understand how you issue certificates to individuals. You did a good job of explaining that. How do you credential departments? It sounds like the end machine that you would be credentialing would not be EHRs, but would be practice management systems or business systems in hospitals. What's the process for issuing credentials to departments and machines?

John Feikema – VisionShare – President
The department head of that, for example, a billing department, is the one who fills out the form and presents and ID to the notary, and they have attested to the fact that they are the responsible party and are allowed to make that determination on behalf of their department and institution. Even the server certificates that are installed at a location have been verified by a specific individual, so we will know. I mean, every single certificate on the network has a person's name in it. They may be functioning as a department head who is vouching for the server that's being installed, but there's still a person there that we can turn to and say, your department is misbehaving, for example. We're going to revoke the certificate for you so that we have someone that we can talk to about that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It sounds like that's true for machines, so your certificates for machines are identical to your certificates for people?

John Feikema – VisionShare – President
Yes.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Any other questions from folks? John, thanks so much. As you can tell, this is a very hot topic, and the questions are getting more and more interesting as we go on.

John Feikema – VisionShare – President
It was good to go as early as I did then.

Jonathan Perlin – Hospital Corporation of America – CMO & President
There you go. Let us move on now to Joe Carlson from Covisint.

Joseph Carlson – Covisint – Director, Data Exchange Services
Hello. This is Joe Carlson with Covisint. I first want to thank everybody for the opportunity to discuss how Covisint approaches point-to-point transfer between organizations across many verticals. I guess a little background, myself and Covisint, we've been doing this for about ten years. We provide our messaging service in a SAS model, integrating organizations across many markets, be it auto, healthcare, oil and gas, and government. My focus is on secure point-to-point messaging.

Within the Covisint platform, we have both the secure messaging services, the portal and collaboration services, and our identity management and security services, which all work together. Just based on some of the conversation I've heard, how we authenticate users and handle provisioning of services is a bit story there that we can gladly tell with a lot of our customers from DoJ and folks in oil and gas, and, of course, auto and healthcare. What I'll focus mainly on though is point-to-point, system-to-system messaging and kind of what we've come across there, lessons learned and, of course, onboarding and success in that area.

What is really secure messaging? It's protocol translation, data integration services, and all the security policies around transport and authentication. Specifically looking at a means of how we authenticate and manage endpoints, regarding our messaging platform, Covisint data exchange services within our hosted application. We manage all of our endpoints. We define trading partners, profiles, if you will, within the cloud for each of our endpoints. We have established trading partner relationships that really drive the flow of data, how we route data, how we manage communication channels, how we associate certificates to that communication channel. So whether we're doing HTTPS, secure FTP, or other messaging protocols, a standard way within the application so both our users and our support staff can manage those interfaces and support them on an ongoing basis.

Within our data exchange services, we enable standards based interfaces, management of the endpoints, as I said. A big part of it is being flexible. How do we enable custom services or non-standard interfaces? A lot of what we've seen is you really have to meet the endpoints where they're at. They have various levels of technology, existing investments in technology and so forth. For us, it's been a matter of being able to adapt to how they do things. A lot of the conversations I start with when I meet with endpoints is understanding their current capabilities. Although we may start down an approach of XDS or HTTPS or NHIN Direct, ultimately it comes back to what they can do today because our goal here is to get them onboard as quickly as possible in a secure manner. Within our solution, we provide the ability, when I talk about protocol translation, that I can connect to an endpoint based on protocol A that really meets their needs, and enable the exchange of data with a hospital, for example, that is more sophisticated, doing Web services and synchronous types of communication. That's all within our data exchange platform or framework.

A little more, just going kind of going through my testimony here, encryption, secure hashing algorithms, all supported as part of standard product. By default, when we do system-to-system messaging from a network perspective, all access is denied. As I work with an endpoint, we go through a collaboration process where we exchange IP information and, based on the protocol, what ports are being used. So first, at the network layer, we allow access IP-to-IP over a specific port, whether it's inbound, outbound. Then once we get through the firewalls, then it hits out applications, and we have an additional layer there that's maybe handling the SSL handshake or further basic author client authentication with certificates. That's kind of the bit there on how we manage a lot of those endpoints security wise.

In terms of how we kind of configure these trading partner profiles and some of the things I mentioned earlier, what's important in our setups is understanding both the transport protocol and authentication criteria. When I talk about channels for each trading partner, I can configure that doctor's office Smith is

communicating over secure FTP, and I provide an interface with all the protocol information associated with that, whether it's certificates, user name and passwords, and so on within our hosted application. It's not something that the provider or the endpoint has to worry about.

Next, regarding an encryption solution, as I mentioned earlier, we support all the standard ciphers, hashing algorithms, and so forth, SSL, TLS transport, IPSEC, VPN solutions. I mentioned in the testimony there, there's a lot of third party sites and open source ciphers and algorithms all supported within our platform. Because this is what we do, we've built the application with hooks that allow us to do everything from SHA, MD5, Triple DES, and so forth, and just really kind of build it into our platform. It's a not a reinvent the wheel every time we come to a new endpoint. It's all part of our base solution that allows us to be flexible and adapt to kind of what the endpoint needs.

Also, under this topic, I mentioned something called our Covisint Scout Technology as a solution that can be installed and configured to run at the endpoint. A lot of times when we're dealing with endpoints, what they'll tell me is, Joe, I have a PMS or an EMR or some other system I use, and I want to send you demographics or receive clinical data and so on. But I don't know how to get it to you securely over the Internet. Our Scout product is basically a simple application, a software appliance that we enable the providers to go to a site. They can download the application. Install it. We gain remote access to their system and, kind of out of the box, it has secure, point-to-point transport over the Internet with Covisint based on an HTTPS protocol. Then we work either on our own or in a collaborative effort with the vendor to establish that backend integration into their EMR, PMS, or whatever system they have through file folders and LLP and other APIs into the backend systems. Again here, our focus is around system-to-system messaging whether we're doing push, pull, and so forth. It's end-to-end access and control of those systems.

Regarding a means of assuring that data is not modified in transport, fully supported, as I said, digital signatures, hashing algorithms within our Covisint exchange link platform used to validate and compare hash values and so forth to understand the data received is what was sent. A lot of standard stuff there. Messaging protocols, you can go down the list of the various secure protocols we support from SMTP with S/MIME and SOAP and REST IO Web services. Again, our focus is around meeting the endpoint based on their needs, so I've listed things. We've done core two for eligibility, PHIN MS, XDSB XEA, doing a lot of work now with NHIN, down to very basic protocols over IP SEC VPNs like MLLP, FTP, and so forth. So it's the idea of really building that pipe first and then being able to kind of manage both ends so that if the hospital is doing something more elaborate, more real time, and we have to build something based on say where the doctor's office is, we can support those.

Of course, part of the messaging protocol solution at Covisint is the Covisint Scout, which I already mentioned, based on the HTTPS transport. We have a whole methodology there on how we deploy it and quickly enable communication over the Internet, so kind of what we've done today. We have thousands of endpoints integrated into our platform specifically within the healthcare using basically our Scout Technology. We have several thousand small offices integrated doing basic demographic synchronization type interfaces to E3 and other applications that go through our messaging exchange here.

Next, regarding a means of confirming receipt of messages: Within our application, it's not just kind of an engine, if you will. There's a complete presentation layer, user interface that really allows complete visibility to tracking of all messages exchanged between endpoints. Then at both the transport and application level, we support various types of acknowledgements and receipts. Whether the protocol level acknowledgement is what we're talking about here where I'm getting 200's back over HTTPS or an LLP acknowledgement or something else, to more elaborate asynchronous type application level acknowledgements where it's not just confirmed that the endpoints receive the message, but they've also successfully consumed it within their application.

The visibility dashboards all available to Covisint personnel and, on occasions, we've also opened up that UI to our endpoints that have more sophisticated staff that really care about that kind of visibility. Typically, a small office would not engage in this type of a looking at the messages at this detail.

I'm just kind of looking through the testimony here. In addition to what I talked about transport and application level acknowledgements, we also support a set of APIs that allow some of our more advanced customers to query status of messages systematically or programmatically within the Covisint exchange, so they can integrate it into their backend systems. They can automate acknowledgements and so forth to really take some of the information that we provide in the cloud and pull it back into their backend systems and expose it through that method.

Next regarding what factors affected our decisions around point-to-point messaging and so forth, kind of really answered this in more what I've kind of seen out there over the last ten years working with endpoints, some of the issues, challenges, and so forth. As I stated, we provide this as a service. Point-to-point messaging can be very costly for many organizations on a continual basis, as the number of endpoints grow.

One of the things we've seen is it's not just about connecting and doing the secure transport on day one. It's what's the real cost of maintaining this on a go forward basis as both the number of endpoints grows, as standards and technology evolves. How do you manage that and be responsive to these changes? What we've seen is really that's a significant task for organizations to overcome, and this kind of touches the operational aspect that I think I heard at the beginning here is how do you really keep it going, not just now or six months from now, but two years down the road? So it's not just the initial investment or onboarding of endpoints, but it's the continual reinvestment in technology that's required here in meeting and implementing new standards. So this is really where Covisint, what we provide as a service, understanding that, working with our endpoints.

Then, finally, on that topic, much of the complexity is not always in the messaging protocol, but it's in the formats and understanding the data, which I think several folks have hit on here today. What we've seen is a lot of folks will say, Joe, I want to do HL-7, and I want to do it over HTTPS or with a SOAP based Web service call. Then when I get into the details here it's, well, we have these slight variations of the standard, and I've modified it and so forth. It all kind of goes back to it's not always as straightforward as I support standard A, but you have to be able to adjust and kind of meet the endpoints on where they're at today on their current implementations.

What do we see as essential requirements for point-to-point exchanges? Focusing strictly on messaging, and assuming the discussions around patient consent and matching of identities and so forth is a separate discussion here. Really the ability to communicate securely over the Internet based on secure transport such as HTTPS, that's where we see a lot of our interfaces, whether it's the standard HTTP operations or messaging protocols on top of it like SOAP and REST IO Web service calls. And so really considering the security and confirmation of delivery are important, but it's also important to build the framework to support the new requirements, as these interfaces develop and standards continue to change.

I already talked about the data, specific formats, and that context. Really, I mentioned there success is in the details. What's important there is the objective here is around onboarding. That's really the criteria for success, how quickly and how many small offices, hospitals, etc., endpoints can I get integrated? It's just not always about the protocol of the transport, but it's really diving into the details and working with typically the vendors more than the physicians at the sites, or getting access to their systems in providing that service to integrate them as a service.

To kind of wrap up here, the exchange of information regarding NHIN Connect gateway, to date the NHIN Connect gateway interface has been more in a pilot scenario as part of HIMSS with the Mayo Clinic and our state of Minnesota health information exchange. We've built the functionality into our data exchange platform along with support for XDSB, XEA, IHE profiles, of course. We have some stuff going on with some hospitals now in Minnesota doing some CCD exchange over XDSB. Then specifically regarding NHIN Connect, Covisint is participating in the NHIN Direct technical implementations with other vendors working to support both the SMTP along with the XDR SOAP based bindings as an onramp for secure messaging, which for us will be another one of our channels for standards that we support.

In conclusion, kind of standard transport messaging protocols are critical to providing directions for organizations and enabling secure message exchange. However, success will be driven largely by the organization's ability to support these standards and how quickly and how many endpoints we can integrate into the ecosystem. So it's important that there are disparate solutions out there and disparate protocols, and those won't go away, I guess, is my point here. We'll need to support NHIN Direct. We'll need to support NHIN Connect, SOAP, and Web service, but we'll also have to be able to support many of the non-standard and custom interfaces that exist today.

This is what Covisint does from a messaging perspective as part of our core service. We help organizations manage the disparate messaging protocols, handle protocol translations, provide visibility and tracking into these message centric interfaces, and then, of course, manage the endpoints and the channels and certificates and everything that goes with that. With that, I thank you for the opportunity and welcome any questions.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Thanks so much. I think we've heard some common themes about each of the vendors we've heard so far offers a transport mechanism or mechanisms with gateway services that may translate one transport mechanism to another. They offer certificate and trust type services, and they offer directory services. Now of course the challenge for the HIT Standards Committee, as we hear each of these testifiers, I suspect that each of those directory systems offered by each vendor is not compatible with another. Of course, these guys that are providing value added services to a variety of customers and endpoints. If we envision a network of networks, a hub and spoke arrangement, I think a fascinating question will be, and I'll just ask Joe this, I mean imagine that a user of Verizon services wants to transport a set of content, CCD or otherwise, to a user of Covisint's services. How we do that?

Joseph Carlson – Covisint – Director, Data Exchange Services
We do similar things like this today. Our endpoints are not just Covisint customers. They're customers of other vendors, competitors, and so forth. We basically engage and collaborate, in the case here in this example, with Verizon. We're talking CCD exchange. We get into basically a conversation, and I'm just kind of talking a little bit how I've seen these go where we start around standards. In this context, we're not really talking HE-to-HE, so we'd probably look at more something like XDS type interface where you have an orchestration of services around patient queries and document lists and retrieval around the CCD.

How we do it is really, it kind of gets down to you have to get in the trenches, and I would work with, again, a focus on this use case, a technical contact at Verizon, understanding their capabilities, their interfaces for CCD exchange. With Covisint, I would say we can support the CCD exchange through XDSB for example. Is this something we can interoperate on? And we'd kind of drive this conversation through.

Then you get into the content. Once you've agreed on some of the transport, then you get into content and how you identify and route and handle this content. Is it going to another endpoint? Is it part of Covisint's, HIE solution where we've integrated our portal services where we have folks accessing a dashboard and, through RLS, we're querying Verizon's system to retrieve a CCD from one of their customers and pull it back into our system. I kind of rattled through a lot of aspects there from the technical to understand the use case, so it's feasible. We do it today. It's a collaborative effort.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Just to maybe editorialize a little bit about Direct, and to elaborate on John's question, the goal of Direct by trying to create an open approach, I'll say standard although it's not officially a standard—it uses standard technologies—would be to enable exactly what John had suggested. If you were on the Verizon network, and you knew the universal address of someone that was hosted through Covisint or through VisionShare or any of the other vendors that are to speak later in the day, the message would be securely delivered, end of discussion. Joe, is that your belief that that's an achievable vision by using something

like Direct protocols where we don't have to handcraft interfaces between every possible N² number of vendors?

Joseph Carlson – Covisint – Director, Data Exchange Services
Yes. It's definitely possible, and I was generically speaking to some of the things we did today around XDS and things. Now specific to Direct, and the addressing, and having domain names and things of that nature, I do think it's feasible, and it's something we're supporting, and hopefully be piloting in January with a group out of Connecticut. Yes, where I tend to do— I guess, after we talk about, okay, we have the addressing, the domain name, and Covisint has this domain name for Direct and so forth. But what's kind of the next steps there or the real use case is, okay, so if I'm a small provider, and I'm going to send a CCD, odds are I'm a provider that really doesn't know how to create a CCD, so I'm using some application, some EMR that I'm just typing into. Then behind the scenes, all the magic happens.

What I'm working to understand a little bit is not as much how NHIN Direct is going to enable secure transport of that CCD, but how are some of these interfaces going to be integrated into the backend applications? Whether I'm sending a CCD or someone is pushing a CCD to me, is it strictly just a view in the inbox type things and that kind of nature? Hopefully I'm answering your question. The short answer is yes, though I believe through the NHIN Direct protocol, they'll be able to push a CCD securely to an endpoint such as Covisint. Yes. Do I think there's more to that picture that's still going on and going to be proved out during the pilots? Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, that's an excellent answer. I appreciate it. One of the distinctions that we made from the beginning of the Direct work was to make a distinction between the edge protocol, which out of necessity will vary depending upon what kind of entity is connecting, and the backbone protocol, which we do believe and hope to have standardized with the S/MIME, SMTP model, which reduces the complexity a little bit. Although, as you correctly point out, it doesn't make it go away. You move the dirt under a set of smaller rugs maybe.

Joseph Carlson – Covisint – Director, Data Exchange Services
Right.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Arien and Doug, any initial comments based on what you've heard from Covisint?

Arien Malec – RelayHealth – VP, Product Management
I just want to amplify that exchange, and I've seen this conversation play out a bunch during the planning for implementation pilots, which is that once you, I don't know if solve is the wrong word, but once you push away the transport piece, the energy and focus goes immediately to content and workflow. I think our hope and aim isn't to have solved the entire problem, but to have swept the dirt under a smaller rug. I like that metaphor. The second observation is that for the Direct Project, pretty early on, I guess midway through, we concluded that the central issues were not around transport. That is, you could skin the cat a bunch of different ways. We had successful implementations with four different transport protocols, and we could have added six or ten, and it wouldn't have changed the situation.

The central issues were around trust and identity, and that much of what we focused on was how to have scalable and common definitions of identity through the use of X509 certificates. In the case that you just walked through, you've got Verizon. We've got Covisint. We've got VisionShare. As long as those three organizations mutually trust a set of route certificates that have the appropriate identity management policies and security policies that are attached to them, what we attempted to do in the Direct Project was insure that the messages could just flow. That is that the key issues were common or compatible definitions of identity, and so to solve that problem essentially and then let the messages flow, so again more of an editorial than a question.

Jonathan Perlin – Hospital Corporation of America – CMO & President

Basically what you're saying, Arien, is if we could just have one approach to trust management, even though that may be a federated approach, of course, and one approach to directory services, then all of these various companies could thrive, connecting endpoints, as they will, offering value added services, but yet still interoperate.

Arien Malec – RelayHealth – VP, Product Management
Well spoken.

Joseph Carlson – Covisint – Director, Data Exchange Services
Yes. I definitely agree, and I guess this may be a point for a broader conversation, but a lot of times what we'll do is we'll start with the use case and the workflow because that may drive the transport. In other words, if we're providing a state or a regional HE solution, it's not about the endpoints pushing CCDs to Covisint. It's about a more synchronous request response interface, which I know is not the topic here, but just the point that the use case and the workflow a lot of times will drive the type of transport interface we built.

Now the NHIN Direct push CCD would definitely probably fit the use case where we want a provider that's maybe feeding a CDR at Covisint that we then turn around and query. My only point there is a lot of times we start with the use case and the workflow. Then based on what we're doing for the larger organization or entity, and then we go out, and we start enabling the endpoints to support that use case and workflow. In Direct SMTP might very well support the specific use case, but we may also need other interfaces that are more synchronous, real time, request response type thing, so just wanted to add that comment.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Well said. This is, as we said, about the whole discussion today is there are many ways you can orchestrate transactions depending on the use case. For the use case of pushing data to biosurveillance or public health reporting lab or immunizations registries or PCP specialists, push works great. It doesn't help you much in the emergency department. It doesn't help you much if what you're trying to do is assemble data from a whole variety of disparate sources where the consent management framework and delivering it just in time.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I have followed Covisint ever since they first came over from the auto industry. One of the early value propositions that Covisint often described was its process for onboarding and determining the identity of end users, so I was hoping to hear something about that in Covisint's testimony today. Joe, are you prepared to speak to that at all?

Joseph Carlson – Covisint – Director, Data Exchange Services
Yes. Sorry. I guess there's maybe a little misunderstanding. I can maybe give you an overview because, again, I was focused on more of the point-to-point secure messaging aspect, system-to-system, that kind of stuff. At the beginning, I mentioned our identity and security services around our trusted identity broker and trusted identity framework solutions. Unfortunately, I could throw some generic terms around how we authenticate and provisioning, and things of that nature, but I don't really have the details myself to provide that testimony today.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If you have such material available, would it be possible to send it to the committee afterwards?

Joseph Carlson – Covisint – Director, Data Exchange Services
Yes.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Are there any closing comments on the Covisint or any final questions?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, kind of following on to Wes, I didn't notice. Do you distribute certificates?

Joseph Carlson – Covisint – Director, Data Exchange Services
No.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Thanks very much, Joe. Very, very helpful. I know, folks, that this is a marathon of testimony, but the joy of doing this virtually is you can go to mute and take that quick bathroom break if you need to. Let's move on to Anand and Axolotl.

Anand Shroff – Axolotl – Vice President, Products
Hello. Thanks. This is Anand Shroff. I'd like to thank everybody for giving us the opportunity to testify before this committee. As you guys know, Axolotl has been enabling health information exchange for over a decade, and you've seen the strategies and standards around exchange evolve, particularly in the area of transport.

We've seen a number of different approaches. We've seen everything from MLLP over VPN, which is what is most widely used today in our systems typically when we are getting data from the edge with edge servers deployed at hospitals, and with physicians using multiple EMR systems. VC secure FTP, the EMR systems or EHR systems are not necessarily able to support MLLP over VPN. Now we're starting to see Web services using two APLS. For systems that are capable of supporting synchronous Web services transactions, this is now becoming an accepted approach and, in fact, we would say that it's becoming a preferred approach.

The combination going forward of Web services, TLS, and SAML 2.0 for endpoint authentication seems to be a powerful one. There tends to be immediate feedback on normal activity. Also, it supports both synchronous as well as asynchronous transactions, which increases the number of implementation choices available.

One of the things called out was encryption, and the VPN, SFTP, and TLS sort of imply encryption. Like I mentioned earlier, a preferred approach is two-way TLS due to its inherent advantages, as well as its evolution from the SSL standard. There was a specific question around end user message level encryption. For that, our approach is generally the PKI approach is adequate. We haven't seen the need to offer anything above and beyond a public key, private key infrastructure.

Messaging protocols, again, like the previous testimonies, there are a number of different candidates that are available: SOAP, REST, SMTP. Restful Web services is personally my favorite approach because they have the advantage of being easier to consumer. Axolotl does support a set of restful Web services. However, there's been no standardization activities around a widely accepted restful interface. We've seen a lot of the standardization work focused on SOAP type transactions through the IHE work, and Axolotl has been a big supporter of the IHE work, and it's starting to get more traction. We are seeing EHR vendors starting to support, but the core--PICS, PDQ, XDSV, and XDR transactions. We also know that IHE profiles are important at the NHIN level.

It's been an interesting situation where there have been a number of different approaches available. Standardization has been sort of absent except in the realm of IHE and SOAP. Now we are seeing the Direct effort with SMTP sort of taking the center stage there, and we are very supportive of that. It has the advantage of using a widely available toolset and, as was mentioned earlier, it's for the little guy to be able to communicate to the little guy, and I think that's an admirable objective, and SMTP is definitely the right choice for that.

There is a bit of a concern that outside of the push use case, SMTP is going to fall short to handle the other aspects. The emergency department use case was called out. It was a concern widely voiced in the NHIN Direct workgroups. I'll just say it again that it basically means that we will have different approaches for different use cases, which is not necessarily the most optimal way of going about building

a vendor supported infrastructure. However, I do recognize that it does address the overall objective of being able to connect small practices, so take that for what it's worth.

The message receipt question that was asked is more relevant to asynchronous transactions and exchanges as opposed to synchronous transactions, in other words pull. In the Web services case, you can use standards such as Web services reliable messaging in distributed asynchronous scenario. We've also used the IHE NAP, notification of availability profile, to enable message availability and receipt notifications. Message receipt confirmations are obviously available in the SMTP case.

What were some of the decision points that we faced? Our original decision point, decision support to go with MLLP over VPN for HL-7 version 2.x was based on the state of the industry, and it was the standard that was achieving the highest level of adoption, so that was sort of an obvious first step for us. For advanced Web services based transactions, application-to-application integration, which we are seeing a lot of, we've obviously supported our proprietary restful APIs, and we are supporting SOAP style IHE transactions with TLS and SAML 2.0. This was influenced by several factors. The primary among them was that IHE was sort of the only accepted or only available standard to describe these exchanges at a detailed level, and the NHIN Connect standards also rely upon IHE support. This played a major part in our decision process.

The use cases that we encounter for P2P exchanges, these are, again, obvious to everybody, but just to go through that inventory, it's a referral use case. It's the transitions of care between provider organizations, typically exchange of discharge summaries. There's results exchange from labs back into the provider system, as well as public health reporting for immunizations and notifiable conditions.

Moving on to NHIN connectivity, we have built and maintained our own gateway that supports NHIN protocols, and we're actually in the process of deploying this that connects the Utah Health Information Network with the local Veterans Administration. We are expecting to see a number of these projects to connect organizations using the NHIN in the next 12 to 18 months. There was a question earlier around how do you exchange information across HIEs or across systems, and the approach that Axolotl has typically been advocating is to use an NHIN style exchange, NHIN Connect style exchange to be able to exchange CCDs.

Another question was around provider directories. Axolotl maintains its own provider directory. We don't support the NHIN Direct protocol today, but it is expected that our provider directories will be able to support that way of communication.

One other question was around real time querying of the HIE for consolidated patient records with the consent management framework. To support this, our approach has been the standard IHE transactions to be able to get at CCD documents using the XDS.V profile. Again, I'd like to thank the committee for this opportunity, and let's open it up to questions.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Thanks very much. I think, again, we're hearing so many common themes about the choices of routing methods. We've heard SMTP. We've heard SOAP. We've heard REST. Each of the vendors have chosen for different reasons to implement a certain type of routing transport standard to meet specific business imperatives, and it sounds to me like all have had good experiences making each of those transactions work for specific purposes.

Let us, again, sort of ask similar questions that we have been asking. You already did talk a little bit about provider directories. But as we get very specific about thinking about how to interoperate a network of networks and having common addressing, you said you did not support NHIN Direct's addressing scheme at this point. But do you envision a yellow pages, a white pages, getting to that nirvana where we'll all have common addressing? What is the current approach Axolotl sees for the future of addressing?

Anand Shroff – Axolotl – Vice President, Products

I think, like the previous answers, I'd have to say that it's all of the above. But I will say that the most obvious answer typically is the one that's been sort of the hardest to accept, which is that a centralized way of managing these things would be a much more efficient way of doing it rather than having a distributed system where you'd have to rely upon HISPs, as well as intermediary points to be able to provide the addressing systems, which is obviously possible. A centralized system, while that may not be acceptable for a number of reasons, is definitely the easiest and the most manageable way to go about it, at least in my opinion.

Claudia Williams – ONC – Acting Director, Office State & Community Programs
Anand, we've had a heated conversation about this in the information exchange workgroup. One of the things I think we've arrived at is a discussion about the difference between creating the obligation to do things the same way, but keeping the information federated versus a truly centralized approach, which bears the risk of disconnecting the infrastructure from the business needs. It would be interesting to hear your thoughts about that. In other words, if everyone used the same addressing approach, and there were requirements around opening up directories and having a common interface approach versus truly centralizing the infrastructure and the data.

Anand Shroff – Axolotl – Vice President, Products
I understand the question. In the second case where you have a federated approach, I think the ability to search for information is still going to be a challenge. It can be solved by having a directory of directories and a number of different steps. But it remains a complex problem to solve, especially with regards to propagating updates, local caches, what have you. A centralized approach, while it does suffer from the single point of failure problem, I think that problem has been addressed to a large extent by having multiple redundant systems handle it. Again, my bias is towards the centralized approach. Neither of the two approaches is obviously full proof or the absolute right answer. But for simplicity sake and for the ability to move the Direct effort forward rapidly, I'd personally prefer the centralized approach.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Obviously this is a great debate in many state HIEs as well. For example, a question we've asked in Massachusetts is if a clinician has five identities because of five practice sites, hospital, Smith, office, etc., might you want a white pages to say here are the individuals. This is all a centralized white pages, which then points you to an organization, and then you deliver the message to the organization, and the organization, once inside its firewall, decides whether it's going to the EHR, the PDA, or the fax machine. That is, it's sort of a combination of centralizing some aspects and federating others.

Anand Shroff – Axolotl – Vice President, Products
Yes. We are seeing states take different approaches. We've seen California starting to ask questions about a central provider directory, and we're doing work in Tennessee where they really want to keep that information distributed within the constituent HIE organizations. It is a very interesting debate. Axolotl does have an opinion, but we're not willing to make a bet at this point.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Arien and Doug, based on what you've heard, questions you have for Axolotl?

Arien Malec – RelayHealth – VP, Product Management
One more editorial, which is that one of the things that we, just on the thread of this recent discussion, one of the things that in the Direct Project we've had a lot of conversation about is the notion of central definition of trust. You may have federated trust, but it's incredibly useful to have a common definition of identity and trust, and it's incredibly useful to have a well-known set of trust anchors that provide that common definition of identity and trust. That may be the federal bridge. It may come out of the … initiative. But that, again, following the theme that transport is less essential than common definitions of trust to the extent that we can get common federal trans-state definitions of trust and identity, we're going to be able to scale up across network transactions much, much faster.

Jonathan Perlin – Hospital Corporation of America – CMO & President

Certainly, as we've thought about directory issues around New England, I mean, currently we have Massachusetts building a provider directory, New Hampshire building a provider directory, Maine building a provider directory. But it turns out, we actually have a fair number of patients across state lines, so how is that going to work?

Arien Malec – RelayHealth – VP, Product Management
And even clinicians across state lines, right?

Jonathan Perlin – Hospital Corporation of America – CMO & President
There you go.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I have another editorial, which is, I mean, I appreciate the importance of directories in the long run, particularly as we move towards perhaps pull services where you need to be able to identify a specific set of people who are allowed to pull a message asynchronously in the future. But in the short run, one of the main reasons that we kicked off the Direct work was, one, to establish the universal address that we've talked about already, but number two was to pattern it after e-mail, which works to send billions, perhaps hundreds of billions of messages a day without a single directory structure. It's the business card directory model. As you find who you need, you know the person that you're sending the message to. You find out their address. You store it in your local system, and that's the end of the discussion. It works very well with very simple protocols, so directories are important, but they're not a barrier to the use of Direct push messaging. The lack of a directory is not a barrier, I should say … my words correct. End of editorial.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Anand, you're talking about the centralization versus federation of directories. I think people often think about the domain name service and believe that there was a time when Deck and IBM each had networking architectures that didn't involve a distributed service. That everybody believed that was impossible. It seems to be working very well and has stood up through some advances in technology. What makes the kind of directories we're talking about here categorically different from the domain name service that would indicate that while it works for domain name addresses, it doesn't work for people identities?

Anand Shroff – Axolotl – Vice President, Products
Wes, I think that's certainly a philosophical debate. But from my perspective, the biggest difference is the fact that you have end users here who will be managing their information. The changes or the ability for individuals to manage that information is easier managed in a centralized infrastructure. Again, this is an entirely philosophical argument rather than a distributed framework with the DNS like capabilities that you mentioned, which is essentially a collection of a server out.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think it's a tribute to one of our testifiers, if we go off and give our own rants because it shows we're at least listening. Let me just say that I pay a particular technology provider $6 a month, and they take care of all that stuff for me, I mean $6 a year, I don't know that the user difficulties in dealing with technology is a problem, or is it a business opportunity for a certain class of technology provider?

Anand Shroff – Axolotl – Vice President, Products
Wes, we also have to ask the question, what is the lowest cost to the small guy?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think we have to balance the approach that says—I've been in interoperability since we were worried about how big the beads were on abacuses, and a month doesn't go by that someone doesn't say, well, here's the solution to interoperability: everybody use our product. There are always practical reasons why that will, in theory, be easier to coordinate and so forth, and yet that's a solution that has limitations of scale, mostly around the power of the vendor in the marketplace. We need to find the balance between what's practical and open versus what is solved more easily by being proprietary.

Anand Shroff – Axolotl – Vice President, Products
Agreed.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Other questions for Anand and Axolotl? Okay. I think what's happening now is we are tiring people out because this has been such a great discussion. Thanks very, very much, Anand, and let us now move on to Cris Ross and SureScripts.

Cris Ross – LabHub – CIO
Good morning. I'm glad to have a chance to be able to offer some comments this morning. This has been a terrific conversation. What I'd like to do in my time here is to describe implementation point-to-point messaging for e-prescribing and how we're adapting that for broad, clinical interoperability. We believe that the models that have been developed for e-prescribing may not be the only model for clinical interoperability, but it's a practical one developed over about ten years, and there may be some lessons learned.

SureScripts maintains what we believe to be one of the largest health information networks today with e-prescribing as its anchor service. The network today connects over 200,000 e-prescribers, 55,000 community pharmacies, the largest PBMs and so on. Today, about 65% of patients in the U.S. are searchable for prescription benefit and history information. The gap from 65% to 100% is largely made up of Medicaid, which is a group of patients that we're adding to the network. We can route prescriptions to about 90% of community pharmacies and do that by certified connections to more than 250 technology vendors, so essentially almost every meaningful piece of clinical technology in use in doctors' offices today is connected to the SureScripts network.

In October, the month recently past, we transmitted over 190 million transactions. At this point, slightly more than 25% of all scripts are transported electronically across the SureScripts network. Part of the reason why we've been able to drive that level of ubiquity in e-prescribing is based on a set of principles that are owners, the pharmacies and PBMs have required that we operate. We've listed them in my written testimony, but those are really around security and privacy. We adhere to the kinds of standards that have been previously discussed today. The idea of neutrality, meaning that essentially all players get to play on a level playing field and get the same access to e-prescribing resources regardless of who they are. We expect to extend that neutrality into how we connect in clinical interoperability as well beyond e-prescribing.

The other issue, one of the key principles is the idea of choice, and that has several dimensions. One is that a patient gets to choose what pharmacy, and the prescriber gets to choose their drug therapy of choice. We also don't do commercial messaging on the network, and our focus has been on enabling our partners, EHR vendors, and others to be able to connect to us in a way that we don't compete with them by providing software for development or sale. Other principles are transparency, collaboration, and quality that are attributes that have made the network work well. That's a brief kind of overview of how we've arrived at this point in time.

At the end of October, SureScripts announced that it was expanding this nationwide e-prescribing network to support and enable electronic exchange of all kinds of clinical information that would include things like CCR, CCD, lab results, referrals, and so on. This network will enable different kinds of connectivity. First, an existing network like an HIE, an IDN, a vendor sponsored network, and so on could connect to this backbone network. The second is that a single vendor or an IDN or a hospital could also connect its system individually to this network. Finally, individual physicians can connect through a secure Web portal, which we'll co-brand with Partners.

There has been some experience in using this network. For two years, SureScripts has supported MinuteClinic in its transport of CCR records to primary care physicians back to the patient's medical home. In that two years, millions of messages have been transmitted. Only a small percentage of them have been transmitted electronically, mainly because the inability of an endpoint to receive these

messages. The key of our mission here is to grow that and to make it able to push messages directly from provider-to-provider.

I wanted to talk a little bit about how we enable point-to-point connectivity. There are sort of two pieces to it. One is that we have a standard implementation to all endpoints. Everyone needs to certify in the same way. In some respects, that looks a lot like the Direct Project or the NHIN Connect or exchange protocols as well. You need to operate on the network using a certain set of principles and a certain set of rules. We think that that makes a ton of sense and it's what's made SureScripts work.

The second is it's a complete implementation. In the Direct Project overviews, there's a description that Direct at this point in its evolution doesn't produce a full sense of interoperability, that that would require transport content and vocabulary, and that Direct focuses on transport, which is exactly the place where it should be. In the e-prescribing world, there's been a lot more codification of content and vocabulary over time, and so there are some lessons to be learned, I think, from what the pharmacy and medication domains have been able to achieve in content and vocabulary, maybe transferrable to what happens in clinical exchange. We believe that when data is put in motion that we'll begin to learn those lessons that can inform what the standards committee is doing in its work.

In the e-prescribing channel of the network, there are a number of central, shared resources like a physician and pharmacy directory, a master patient index, a routing engine, a contract management validation, translation, audit trails, connectivity message reporting, and so on. There are some other services that are provided by the e-prescribing backbone like formulary files that are propagated and stored locally, and there are also specialized nodes on this network like a PBM, which holds prescription history and benefit information so that that look up happens on a federated basis rather than a centralized basis. Finally, there are also aggregation nodes on the e-prescribing network, so most EHR vendors actually manage e-prescribing hubs on behalf of their customers. In other words, SureScripts may not connect to every specific instance of a particular vendor's application, but will connect to that vendor, who then propagates e-prescribing out to its members, and that aggregation model has served that network well from the standpoint of reliability, efficiency, and so on.

You asked questions around authentication, encryption, and so on, which I've included in written comments. I think our answers will be almost the same as everyone else who has spoken today. There's some consensus on standards, and some local variation, but the industry is, in general, driving towards more common implementations and less particular implementations.

What I'd like to do is to spend the few more minutes that I want to talk about the specific questions that you asked like what factors affected our decision to implement P2P messaging, as we did. The simple answer is that we designed P2P messaging for e-prescribing around the business requirements. In the e-prescribing environment, there were business requirements that called for bidirectional, synchronous kinds of communication, and because of that, we built a network with backbone elements to support that. We also implemented a restful implementation to harness those central shared resources, as well as to support the kind of bidirectional synchronous messaging that was required.

If you walk through the series of messages that are required to initiate a medication, an insurance lookup, a medication history lookup, a query about formulary, a local check against a drug database that looks for drug/drug, drug allergy interactions, those kinds of things, then a lookup of a pharmacy that the patient chooses, and then the propagation and transport of a script. If you look at all of those transactions that are required to happen in the context of a patient's visit to a physician's office, all those things need to happen in a matter of a few seconds, a minute at most, maybe two minutes. There's a significant amount of bidirectional synchronous messaging that needs to occur to make that work. It's simply required for e-prescribing, and so that's the way our network works.

We intend to connect our network, the clinical interoperability network, to any other qualified network that would meet the conditions for participation, the ideas of openness, neutrality, and so on, and we fully expect to connect to the Direct Project networks and to NHIN Connect networks. We believe that we will originate users on the SureScripts network for clinical interoperability on the basis of a couple of things.

For example, ease of connection to a single pipe for both e-prescribing and clinical interoperability, and then also for value added services. We think that local networks may connect to our network because of those value added services, but we believe that we're strongly complementary to existing network and emerging networks like ones that will be built on the Direct Project. We expect to connect to those networks on a peer-to-peer neutral kind of basis, including providing a gateway to Direct Project with taking advantage of universal addressability and so on. I look forward to the questions we may have around how directories work on all the rest in that space.

You asked what do we consider to be essential requirements for simple, point-to-point exchange. The requirements really again depend on business requirements. In the instance of where it's a simple push to a known directory using the kind of business card directory that David McCallie talked about, then the very clear, clean, simple protocols of Direct Project may be not just good enough, but in fact complete. But if the requirements are more complicated, for example, exchange between multiple parties where parties may not be known to each other, where a directory lookup is desired, where there's complex message delivery, bisynchronous communication requirements, addition of unknown parties over time, query or reply from some form of index or data store like a medication history, database, or a formulary. Those kinds of requirements then we think more complicated or complex technology may be required.

To return to, I think, what is the key theme for today in this more complex scenario, we think the key is the presence of a trust model where trust can mean security, which is both the process of how does a person get a certificate or a credential. Then what can they do with those credentials to send and receive messages, and do I know that who it is who is sending me a message is really who they say they are? When I send a message to someone, I really know that that's my intended recipient. That's a place where trust in directories are going to make a critical difference.

Trust can also mean integrity, meaning that if I send a message to an endpoint, can I trust that it's going to be handled in the way that I expect, that it actually will end up on the desktop of the clinician of importance to me? It also can mean, trust can mean capability certification, meaning that if I send this kind of message to this receiver, will they be able to interpret it, and can they consume that message in some meaningful sort of way? In this instance, we really hope to stay pace with the standards and approaches that are implemented by the policy and standards committee, but we also believe that practical experience across our network and other networks is going to be a learning environment that should inform what the policy and standards committee thinks about.

Finally, do we exchange information with federal organizations using NHIN Connect? To date, we have not since the e-prescribing network has not extended to federal agencies like the VA, DoD, or others. But we expect that to change. As part of our IHE integration work, we expect to support the CONNECT architecture and CONNECT payloads, as well as connecting to the Direct Project. I think I'll complete my comments here and look forward to your questions.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Thanks so much. Just as we have with the other presentations, we heard this important discussion of directories, trust, and transport where just how important it is to have a common mechanism for directory management. Certainly as we've asked the others about the interoperability of their directory schemes, I'll ask you the same. Creating trust fabric that enables through a federated mechanism the trust across networks and transport, well, it does seem as if the folks at SureScripts, although internally much e-prescribing is done with a restful approach, that you're committing to use the SMTP, S/MIME approach via a gateway. That you are also committing to use a SOAP based approach to interact with the NHIN CONNECT so that you are using each of those three transport mechanisms, but deriving a single trust and directory approach that you're laying on top of three transport mechanisms. We'd certainly love to hear your thoughts on interoperability of your directories.

Cris Ross – LabHub – CIO
Your description is accurate. The issue with directories is to be determined, as we pursue initial connections to the Direct Project. The idea of a universal address does not mean a universal directory. We can have a universal naming standard, and if I happen to know Dr. David McCallie's NHIN Direct or

Direct Project address, I can certainly address him if I am a physician that's on the SureScripts clinical interoperability network where I have my address in that environment as well. And Dr. McCallie can send a message back to me. But I may not be able to search a directory and find Dr. McCallie in a way that I might be able to find Dr. Halamka if he is on the SureScripts directory.

I think the issue is going to be how do we connect between directories. Our approach and suggestion is a way to have directory exchange so that if there is a network that connects to us that there's a way to receive credentials or receive information, excuse me, around that directory so that it could be searchable from within our domain or any other domain. Is there a protocol for exchanging directory information today? I don't think so. I think we're going to have to figure out how that works. But it is also the case that our anticipation is that someone who is on the network that we're maintaining would be able to send outside the network to any known e-mail address. The model for verification of identity is going to be important, and now that the reference implementation work is done, we expect that that engineering work is going to continue.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Let us open it up to others who have questions for Cris.

Arien Malec – RelayHealth – VP, Product Management
I actually had a question as opposed to an editorial. It occurs to me that in the SureScripts network or, rather, the e-prescribing network and formulary and benefit network, the development of that network has been characterized by a few larger players that had been able to—you get a different trust network, and you get a different set of standards for harmonization in that environment. It's not unusual to electronic prescribing. It's the same thing in credit card processing in the financial industry where there are three large card issuers. You see similar kinds in automotive, I guess, with Covisint. You see similar dynamics in other industries. In the clinical exchange world, I think, on this panel, we have more large networks, if you will, than exist in the area of pharmacy aggregators or PBM aggregators in the electronic prescribing area. I'm wondering how those network dynamics and network topologies informed the trust and standards that SureScripts used and how those may need to change if you've got a much wider variety of networks that are participating.

Cris Ross – LabHub – CIO
Right. It's a great question. I think the issue is that there are both nodes of high concentration and low concentration. For example, within the PBM world, a limited number of pharmacy benefit management companies. Fifty or less manage prescription benefits for the country. If you can connect to the large three or four, you've accomplished a lot of that connectivity.

The same thing may be true for the chain drug industry as well. There are a limited number of very large chains that are a significant part of pharmacy. But it's also really important to know that the community pharmacies are significantly large, as well as the chain drugs, and so we're connecting today to lots of individual drug stores managed by individual proprietors where their interests are represented by the Community Pharmacy Association, the NCPA. Likewise, most e-prescribers or many e-prescribers are in an ambulatory setting and, as we all know, most ambulatory physicians are practicing in small practices. Part of the magic there has been that the vendors who serve those providers have provided aggregation services so that, to pick a vendor at random, eClinicalWorks or Cerner or anyone else, is providing an aggregation service on behalf of their individual prescribers. So that the individual doctor's office is not maintaining the technology required for managing uptime of the network and remedying service issues and so on. The EHR vendors are doing that on behalf of those individuals.

I think, if we are looking at an extreme of where individual physicians need to manage all of the infrastructure and business process around connecting themselves to all their peers, that's an awful lot of overhead to be imposed on a small practice. In reality, I think, the industry has generated opportunities for vendors and so on to provide those services on an outsourced basis to individual providers. They buy the software from a vendor who then performs services for them. I expect we'll see the same thing outside e-prescribing. We've heard it today from these other vendors and ourselves around how we're

looking to try to take over that job for clinicians because their job is to treat patients, not to manage technology, and we think that we can do that.

Arien Malec – RelayHealth – VP, Product Management
As a brief follow-up, it sounds like you're saying that one of the things that made particularly in the pharmacy world connectivity scale is the existence of natural aggregation points. For example, for independent pharmacy, the manufacturers or the providers of the pharmacy software systems often provided proprietary networks that could then be cross connected, and it may be the case that in the clinical connectivity world, EHRs, HIOs, other kinds of organizations can offer those same kinds of natural aggregation points to help reduce the network-to-network connectivity.

Cris Ross – LabHub – CIO
That's exactly right, Arien, and every conversation we have is always interesting. I guess if I were to put a bet down, I think our SureScripts bet here is that this will be a peer-to-peer network with lumps. It won't be a completely flat fabric, that there will be emergence of the kind of aggregation points you just talked about.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Other questions for Cris? Come on, Wes and David. Nothing? Very good. Thanks very, very much, Cris. Certainly as you build out this network that you're embarking on, look forward and wish you the same success you've had with e-prescribing.

Let us now move on to Eric Dishman and Garry Binder from Intel. We'll be hearing about devices and their experience with transport standards.

Eric Dishman – Intel Digital Health Group – Director Health Innovation & Policy
This is Eric Dishman. I'll start us out here. Thanks for the opportunity for having us. I imagine you East Coasters are starting your lunch now, so we're a little jealous. We're finishing our breakfast here on the West Coast. I would also thank you for doing this virtually so that we could participate without having to go through the TSA pat down at the airport right now, so very much appreciate you using connectivity technologies to do this.

I should give full disclosure. I run healthcare innovation and strategy for Intel, but I'm not an engineer and not an IT guru. I'm a social scientist by training and bring that perspective to the discussion today. Until I had to prep for this testimony, I really thought that SOAP was something you used in the shower, and REST was something you don't get enough of working at Intel, so I have brought Garry Binder along with me today. He's a senior architect in our disease management group. He's been working on sort of secure data exchange back from being a primary author of the Rosetta Net implementation framework to more recent work we've done at Intel on getting our Intel Health Guide product in the home. And the software there to help connect endpoints in the home and consumers in the home to be part of the care network. In fact, I was particularly heartened this morning when you started the conversation talking about making sure that we include use cases that include the home and family members and perhaps community health workers. And a range of devices, some of them medical devices, and some of them that are going to be consumer devices as part of the mix that we're going to be needing to anticipate and build an infrastructure for going forward.

Intel is probably a little bit in a different situation here than some of the other vendors here at the table. We're not really a healthcare company per se, notwithstanding our upcoming joint venture with GE and the work that we've been doing on home health and Intel Health Guide, which is about to spin out into a joint venture. By and large, sort of Intel core as a company has been working on healthcare innovation worldwide, even though we're not really a healthcare vendor per se. My own social science team at Intel has done about ten years of field work studying now about 250 healthcare facilities in 20 different countries, large and small, trying to understand and, in many of those, been studying their adoption or lack of adoption of electronic health records over the years, and continue to do that work now.

We certainly have helped do architectural work with the NHS Spine in the U.K., similar efforts in Canada working with the Chinese Minister of Health for the regional health information network now and continue that work in Australia. We certainly work on these kinds of issues from small issues of data transport to sort of large issues about how do you deploy broadband in communities effectively, and sort of all points in between. How do you sort of architect from sort of the body in the bedside all the way to the clouds and make sure that you have secure data exchange amongst all those pieces?

We're actively supporting NHIN Direct. I had just grabbed Rick Cnossen, who's the president and chair of the Continua Health Alliance, given some of the questions you asked this morning, and pulled him in. If we want to talk a little bit later off script about the HL-7 personal health monitoring spec that we've been working on with Continua, we can certainly do that. We're certainly baking some of these security technologies such as AES for encryption right into our hardware on silicon itself so that every touch point starts out encrypted and sort of maintains that sort of all the way through the network.

Lastly, we're doing a lot of work with healthcare providers in the U.S. right now, more than a dozen of them on their sort of IT strategies and blueprints for becoming an accountable care organization. What I would say to you in that work is, we're seeing a lot of attention and momentum around making sure that their campus and their clinicians are connected. Part of what we're instigating and trying to make sure happen is that both their consumers and their communities are connected as well. That does mean pushing these end points out to the home and into the community in some ways that our use cases might not have anticipated and definitely changes the design and the topology of the network. Particularly, changes the workflow required both from patients and for some of the clinicians who are caring for them.

At a high level, I would say we echo what many of the other folks here have already said to you today. I think Arien said very nicely earlier, and we agree, that the central issues are around identity and trust, not necessarily the transport. Nonetheless, you've asked us to focus on today on what we do in transport, so we'll start with that.

I'd say the second point is we believe, and our own experience has shown, that secure data exchange between healthcare providers of any size is doable and achievable. The third point is that there are several standards, many of which you've heard talked about today and we'll echo again here from PKI, to SMTP, to AES, and others of this acronym soup that I admittedly did not even know until we prepared for this testimony. I hope that you never expose most doctors and nurses to as we try to get these things adopted, but we think there's many of these standards and capabilities that are available to really flexibly fit the needs and use cases of particular providers.

Size will make a difference. Degree of adoption of IT will make a difference. Rural versus urban may make a difference, and their cultures of trust about workflow and share ability of data within their environment will make a difference. So all these tools are going to need to really fit the unique needs of a provider, but at the same time if we have an infinite number of standards, we're not going to get very far in terms of being able to speak to one another.

With that opening perspective, I'll turn it over to Gary, and he can give some very practical examples of some of these points with our experiences with implementing these kinds of systems.

Garry Binder – Intel – Senior Architect, Chronic Disease Management Group

I want to thank the committee and the chairman as well for the opportunity to provide this testimony. Thanks, Eric, for the good overview. We really have spent a lot of time implementing B2B at Intel or eCommerce solutions, to use a '90s phrase. But, we've also done some work recently with a point-to-point solution and primarily with our health guide product, landing an end point within a patient's home and transmitting information back and forth between that point in a central repository and even on into an EMR.

Let me address the transport question first, the SMTP, the SOAP, and the REST. Let me just say right off the bat that we use Web Services extensively in our solutions and very much support their use. As a software engineer, I understand why SOAP and REST are very useful, very popular. As an architect, I

also understand the benefits of them, and as a systems integrator, also understand why we really like to have those real time data transfer capabilities in place.

I think if we took a survey, I think four out of five physicians would probably say that, as Eric said earlier, SOAP is something you wash with and REST is something you don't get enough of. What we're really looking for I think from a clinical perspective is how can we get data in and out of our environment effectively, quickly, without interruption, without downtime, and certainly without having to have any in depth knowledge of a breach notification process for example.

The point is, is that we really look for these things to be utilitarian in nature as I want to treat them as plumbing; I don't want to have to know what it is. Given that, I think there's a wide spectrum of transports that really come into play. They seem to have a strong correlation to the size of the organization that you're exchanging data with; from the very, very large where you have a VPN in place, database replication, to medium and large who embrace a SOAP or a RESTful architecture. To a small to medium where SMTP maybe the best and is often the best protocol to use for exchanging data, down to what we deal with on a very frequent and daily basis, getting data out to a patient. That's something that has some additional challenges, because it's not a small organization, it's a nanoscale or an individual organization.

In many regards, that particular end of the spectrum is interesting, because we're often faced with end points, which don't even have a routable IP address for example. They do have IP addresses, but they're not routable because they're in a home. So using technology that are related to SMTP, such as POP or IMAP to go that last mile, that last leg of the trip sometimes is necessary. We also use some technologies that have come out of the instant messaging world, such as COMET or BOSH to push that last leg and push data out to the end point, and this is at the very smallest end of the spectrum. For the most part, I would expect that what we consider small and medium organizations, SMTP is really going to be the most widely acceptable and most ubiquitous protocol that can reach there. Like I said before, it does have that advantage of having the additional POP or IMAP last leg if needed in the case of a very, very small organization.

The one thing that we mentioned in our written testimony here is that while SMTP is probably one of the most ubiquitous, and we have talked many times about the billions of messages that are successfully delivered every day, there are some real basic limitations. We've talked about one of them already in the sense of in the urgent message, their maybe some delay in the delivery. Also, there may be some restriction in terms of size. So if we're going to be sending messages that are medical imaging, those sorts of things that can get into the tens or hundreds of megapixels, they're maybe some limitation. We may have to address that using technology, such as splitting up the message or making sure that we have appropriate configuration within the infrastructure to make sure that those things can be delivered.

In general, what I'll say is that SMTP, while often known as the e-mail engine, also works very well as a point-to-point protocol in a number of other industries. People are probably aware of this, but a number of other industries have used this at length to send EDI documents in a site, specifically a standard AS1, it's RFC 3335, which talked about sending EDI messages over SMTP and using S/MIME for a liability and for privacy. It's actually gotten quite a bit of play in that regard, and I think field proof that it's a good way to exchange messages.

I'm going to move on here to authentication. I agree with the direction, and there's been quite a bit of discussion about PKI, and I'm not going to go too deep into that. The one thing I will add with regard to authentication of end points and message integrity is that there's an ongoing philosophical discussion to some degree about the granularity of digital identities. There were quite a few questions I think today about where we assign—what level of organization, individual system that we assign digital identities to.

I think there's two rules of thumb, and I think the first one and most important is that a digital identity should ultimately and accurately reflect the sources of data. So for example, if the data is a message from a doctor to, for example, a patient, I would expect that that message be signed with the doctor’s digital identity. If it is a message that comes including a lengthy history of the patient for example, I would

expect that message to be signed by a digital identity that's given to the EMR, the system that houses that data rather than an individual. I think that's the first basic rule of thumb is we want these, as a healthcare consumer, I would want these things to, these identities to be assigned based on the nature of the data being sent.

The second thing is, is that granularity and moving these digital identities out to the end points does make some good sense, and it should be done using common sense and reason. We certainly don't want to move to the point where every individual is required to have a digital identity when that doesn't make sense and when there is an infrastructure to support that. However, moving in that direction as time and technology allow does add some value and like I said, that does not trump the first rule of thumb, which is the signature should and the digital identity used to generate that signature needs to accurately reflect the source of the data. We absolutely, like most of the other members here today, support an end-to-end digital signature. This is something that I think is very commonplace in business-to-business transactions today. I would expect it to be so in the healthcare exchange as well.

Let's go on: Eric talked about encryption a little bit already, which is awesome. I think there's been a couple of different positions put out today. One is the discussion and the use of TLS for encryption. We really support that technology for a link level encryption, and I think it makes good sense to do it. It's very widely used. In the industry, it performs quite well. It provides all of the privacy that's needed, the confidentiality, even for header information and so forth, and not to say that end-to-end encryption isn't necessary in some cases as well. What I would say is while link encryption might be a good minimum standard, we wouldn't object to anyone who said, "You know what, I really want to have end-to-end encryption on my message as well, and I have good reasons for that." I would certainly say that's acceptable in exchanging the data.

The last area that we were asked for some input was on message confirmation. This is acknowledgements. This is an area where in the past, an involvement that Intel's had with a number of standards efforts, we've learned. Not to the point where we're ready to admit mistakes, but we would certainly do it different in the future. There's a couple of cases where acknowledgements basically have been inferred from either a higher or a lower level in the stack, and I'll give you a couple of examples. One of them is inferring an acknowledgement from a lower level in the stack is basically taking a two hundred okay from an HD to be opposed or good, and inferring an acknowledgement from that, and that's a fairly common practice.

Another one would be or at the other end of the spectrum is inferring acknowledgement from a higher level in the stack. This would be in the case where I make, and I'll use a purchase order example, but I'm sure there are others, but I make a purchase order, I send it over, and instead of a message level acknowledgement or a functional acknowledgement, I get a purchase order acknowledgement back, which is at a higher level in the stack.

I think it's critical that in developing and writing a standard, we really focus on getting functional acknowledgements as a required part of that standard. That would be really having the equivalent of a 997 that was mentioned earlier from EDI X12. Or, a Web Service reliable messaging type of implementation that's going to give us a real functional acknowledgement from that system and not be tempted as other standards have been to allow people to skip the functional acknowledgement for a higher level acknowledgement or a lower level acknowledgement.

We really think that digital signatures are ubiquitous enough where using a non-repudiation of receipt in that acknowledgement really makes a lot of sense. It really cuts down from a system administration perspective on the overhead of having those conversations with their partners in different companies about, "Well, I don't know whether I sent it or not," or "Can you resend it," or "You didn't send it," or those kinds of discussions. Basically, they become completely eliminated when you have a use of a good acknowledgement system, so certainly support that.

Let me wrap up here with a couple of, answering a question about what you consider essential requirements for simple P2P exchanges between two provider organizations. I think the key and most

important item here is, let's build whatever solution we have on existing known standards. The reality is, there are different levels of standards out there in terms of quality. Let's carefully choose the standards that are going to meet our needs, that are going to be simple, that are going to be clear. I've seen this material on the direct Web site, and I applaud the use of the language that's out there about applying technology as needed and staying away from the speculative generalization that sometimes happens.

The second thing is obviously and we've talked about this in the PKI based solution is not only for message integrity authentication, but also for the non-repudiation of receipt. I think it's an easy technology to implement and require to serve all those purposes. Then SMTP, we certainly support the use of SMTP for reaching those small, very small and medium sized organizations or individuals, and the associated protocol such as POP, S/MIME. In the cases where it's appropriate, SMTP over TLS, and there's some standards out there that explain in detail how those implementations are done, and they're fairly commonly available. Then finally, obviously supporting the encryption, and Eric talked a little bit earlier about how the encryption technology is important to Intel so much so that it's worked its way into the actual silicon of our processors to provide a very fast mechanism for providing that confidentiality and protection that's needed for the data.

Those are the essential requirements. Of course, as we get outside of the realm of what we consider essential, we can provide hundreds of more, but those are really the key items. Building the solution on standards is by far and away the most important, keeping it simple and deliver it, and making sure that we have something that provides the widest degree of interoperability as possible.

John Halamka – Harvard Medical School – Chief Information Officer
Great, thanks so much for your testimony. I definitely applaud your comments about functional acknowledgement. I was using an eCommerce site the other night, and of course, my expectation these days is that you will go to the Web, you will do your transactions, and then an SMTP message will be sent to you acknowledging that you completed your transaction. The Web site simply said, "Okay, you're money has been transferred, have a happy day," and no functional acknowledgement, i.e., an SMTP transaction occurred. So I now just have to hope in a week or two, the product arrives.

Garry Binder – Intel – Senior Architect, Chronic Disease Management Group
Well, it's funny; Cyber Monday must have been too busy for most of the commercial Web sites last night. I just logged in an hour ago to see if some of the purchases I made yesterday actually went through. I resonate with that.

John Halamka – Harvard Medical School – Chief Information Officer
Let us open to questions for Intel. Arien and Doug, things that you had heard?

Arien Malec – RelayHealth – VP, Product Management
Yes, I really appreciate the testimony. I'm going to ask a highly leading question and I apologize in advance. I'm going to pop up one level of this discussion to the concept of a universal address, John, what you called a healthy world and a universal method of transport or at least a common method of transport. The implications for the device world, where if I've got as a consumer, the means of having an address that is mine or that maps to my data home or to my personally controlled health record. If I've got the ability to enter that device into my scale or into my glucometer or into my blood pressure cuff or what have you or the chip in my shoe or whatever, does that radically change the world of medical devices? Is it helpful? Is it useful, and basically just interested in your take on that? Then interested in your take on what are the identity trust preconditions for that kind of world?

John Halamka – Harvard Medical School – Chief Information Officer
Okay, let me repeat the question and make sure that I've got it. At the highest level anyway if a user has a universal address and they plug that into a medical device, does that dramatically change the device industry, is that the—

Arien Malec – RelayHealth – VP, Product Management

Yes, does it change the ability for me to take a device that I own and couple it to my own choice of personally controlled health records or send it to my provider in a way that's simpler than the world that currently exists for getting data to providers or to my own personally controlled health record. That's question one. Then question two is, what are the trusts and identity preconditions for having that world?

Eric Dishman – Intel Digital Health Group – Director Health Innovation & Policy
I think part of what we're seeing already, and actually, I just grabbed Rick to join us as well from Continua. He's been sort of in the throes of these issues as well. Part of this is going to depend on whether or not the data is going directly to a clinician be it that interface. Is this an FDA cleared device, is this an approved medical device, or is this a consumer device? I think we're going to quickly come into a world where levels of trust are assigned and assumed depending on the answers to some of those questions.

We already sort of see this with the PHR debate today about is this "real" health data, because it comes from the electronic health record from my doctor or is it not real health data, because it comes from my personal health record. Then an addition of a range of devices, some of them medically approved peripherals that are trusted for what they capture and others more self-help peripherals. I think there's going to be the need to identify those data sources, and there's when we need to build some of the data architectures.

Rick Cnossen – Continua Health Alliance - President
Hello, this is Rick Cnossen. I'm the President of Continua Health Alliance. Eric asked me to jump in here real quick. I just wanted to make one comment. When we in Continua went and wrote the standard to integrate personal health data into the electronic health records, we worked inside of HL-7 in the CDA group. We put in place a standard that—if you look at the end-to-end perspective, it stores data that says, what is the model number? What is the serial number? Is this regulated data or not?—with the notion that the systems that are consuming those data would know what they're intended use are and the quality of data that they require, and they can choose to throw the data out or not.

If it's something that requires data from a device that you've already validated with and you know it's being calibrated and regulated, you should be able to understand that and say, yes, this is data I can trust or it's not data I can trust, and throw it out. Whereas, if it's something that just is a record of someone's personal vital signs that they'll give it to you verbally or they'll give it to you electronically, maybe that system can go ahead and use that data. I think we tried to accommodate, at least in Continua's standards, information that would allow the consumer of the data to choose to trust it or not.

The last part of the question as I recall was about the security and identity, digital identities or digital signatures related to that data. I think there are some current limitations in the industry—or perceived limitations in the industry—about a device being— This is kind of the difference between a cell phone and a smart phone. Many times these devices have enough logic to transmit their data over a serial connection, whether it's wired or USB or Bluetooth or IR or what have you, and that is about it. I think one of the things that we're going to need to see going forward—and not only to support the Continua effort, but also to support these higher levels of authentication—is the equivalent of a smart device or a smart phone where you have more logic, you have the ability to, and whether it's including a TPM as part of the solution or what have you. Currently, the industry to some degree is still in the timeless cell phone kind of mode, and we need to move them a little bit further towards the timeless smart medical device.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
John, this is going to stray a little bit, and if you want to use your prerogative to call it back, that's fine. I'm trying to think of the implications of home health broadly on Internet issues, including those that we're addressing today, but beyond them. I know that you've worked extensively in home health among the three of you there. I'm seeing a vision in some statements from some vendors about unattended home health, that is home health where there is not a licensed clinician there, requiring extremely high bandwidth and extremely high guaranteed response time, so a very high quality service. I tend not to think that. I'm curious what your vision of development home health is with regards to say the level of networking that you have for instruments in a hospital or something like that?

Garry Binder – Intel – Senior Architect, Chronic Disease Management Group
There's a couple of factors that are involved in answering the question. The first one really has to do with what class of device do you have? If it really is a monitoring device, not intended for intervention and critical situations, then you have some options. The reality is that our product supports a subset of the functionality over a POTS line for example, which is obviously not the preferred way of deploying the solution, but we also support connectivity over 3G. I can tell you that 3G is not necessarily the most robust, although it does have the ability to exchange data quickly, depending on your distance from the tower, that whether the 1960s television is close to the radio or the microwave is on or the steel door is open, and those sorts of things. Broadband obviously has some benefits as well.

By the time you get into 3G/4G space, you're starting to get to the point where you can do some non-diagnostic video conference calls. Certainly over broadband, you can do the same sort of things. I think I'm in hearty agreement that it's not necessarily required; however, there are significant benefits as you increase the bandwidth.

Rick Cnossen – Continua Health Alliance - President
I'll throw a few words in there too. I think as you start getting video and video interaction and increasing a richer experience, some of those items are going to increase. But John, I think you and I, I remember last, I think it was about a year ago at Christmas time, we were talking about different models in a home, where one was a model where it was consumer based and consumer facing. The other was taking acute care equipment, putting it in the home where the clinician is directing what goes on there, and you needed a nurse to operate it.

But in the home health quite often when we look at the big diseases that home health are being used for, like chronic heart failure, diabetes, obesity, and hypertension, you don't need streaming real time data. Certainly, in Continua and the implementations we found for treating most of those chronic diseases in the market, you can get by with sending discrete data elements. The pulse oximeter is probably the one that has the most demand. Even there, we get by with doing something that's near real time. We don't send streaming data, but as we grow and look for more of the acute care in the home equipment, maybe the demand for streaming data real time is going to increase. I think we need to differentiate just a little bit.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So would you then support the argument that there's the need for a carve out in net neutrality for home healthcare?

Eric Dishman – Intel Digital Health Group – Director Health Innovation & Policy
We've had these conversations as part of the national broadband plan and certainly worked on the healthcare chapter in that and then said, we don't need it immediately, but you extrapolate out to a future. We're already doing work in places like South Korea where they have a much higher broadband network, and they're doing multiparty patient/physician/family member HD level video conferencing, and real time monitoring of in home cancer care equipment. That's an extreme usage model out in time that will someday become commonplace.

In that future, you're going to certainly want to have the ability to prioritize bits that are related to a heart monitor and making sure that that data gets to its location with some priority over the recipes that you're sharing with your mom. I don't think we need that right away, there's a lot of low hanging fruit that we can do for chronic care management. As Rick said, that just use the networks that we've got to do basic vital signs capture, basic video conferencing that are a huge improvement for doing electronic care today. But certainly out in time, you're going to see the movement of everything from home dialysis—home dialysis is already there, but you're going to see home infusion increased for cancer care and other kinds of things, where that level of robustness and immediacy for data, and certainly continued security are going to be important.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I think that the fundamental question really in terms of predicting this is, when will you be doing interventions that are on a patient that fragile without a licensed clinician being present? What I'm really arguing or trying to get straight is whether this use case of you can really do things remotely when nine of the ten interventions you might have to take on if things go south require someone there to do the intervention. Sure, you can adjust the infusion pump, but if the danger is immediate, are you really going to do that without a clinician around. That's really kind of—

Eric Dishman – Intel Digital Health Group – Director Health Innovation & Policy
We have a kind of segmentation model that we use that says what's reasonable for an empowered patient to do a loan. Now, there's another model that says, what role can community health workers, who both virtually and in the home, what about actual licensed clinicians in the home and what about actual licensed clinicians virtually? I think there's a mix of use cases and models that you can look out and you have different needs. That's true today. We're already doing home infusion and home dialysis today without a licensed clinician present, but we don't have very good and effective monitoring of those systems today, often for vital signs and other kinds of things that you would want, that would add degrees of confidence and safety to it.

As we think about the use cases, we may need meaningful use stages for home based care that start with the real simple low hanging fruit, less real time, less invasive and less dangerous kinds of use cases, but out in time I think it's reasonable to expect. In fact, I think we're going to have to do it from a resource management perspective that the home is going to have to increasingly become a place of care, where it's going to be a mix of in home, in clinic, and virtual visits. What's the platform and security architecture that's going to support that?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
And so that we, in terms of we have use cases with Continua or Intel—

Eric Dishman – Intel Digital Health Group – Director Health Innovation & Policy
Both, yes. These use cases are born out of the field work that we do, and we study a range of segments of home care. A lot of those use cases have said it—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
No, I should be more specific, the speaker, who is speaking was from, there are three of you there and I don't know your voices.

Eric Dishman – Intel Digital Health Group – Director Health Innovation & Policy
Yes, sorry, that was Eric speaking from Intel.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Okay, thanks.

James Walker – Geisinger Health System – CHIO
I'd just add to Wes' comment. We will need a smart extensible architecture no question, but we are very far from having high quality studies that demonstrate, that even the simple remote physiologic monitoring for the basic diabetes and heart failure are effective that we just recently paper published. We're just going to need to be very smart and it may not be this committee's job obviously to really validate in clinical trials that these things are safe and effective, and particularly for any significant number of patients.

Eric Dishman – Intel Digital Health Group – Director Health Innovation & Policy
We certainly don't disagree with the need for spending some of our comparative effectiveness dollars and other kinds of resources to do these comparative studies. What you want to caution is, and we've seen this historically over the last 20 years of work that's been done at Intel Health and elsewhere. You'll see a particular study of a particular technology and a particular use case that may not have born through, but we throw the baby out with the bathwater for the whole class of in home and in community technologies.

We're going to have to come up again with these kinds of phase models and these segmentation models so that we know we're comparing apples to apples when we make these claims about what does and doesn't work in the home and in the community. From a strategic standpoint, we at Intel are working with many governments around the world with the belief that there simply aren't going to be enough resources to not do this. That driving a home and community base infrastructure and care strategy apart of national security and viability for our healthcare systems and economies going forward, and I hope the U.S. is going to adopt that position as well.

John Halamka – Harvard Medical School – Chief Information Officer
Other questions that we have with the folks at Intel and Continua?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I want to get back to the more mundane. I wanted to clarify something that when I read your testimony, and first of all, I want to tell you that you've written testimony, as well as the verbal, but the written was really, really well done, so thank you very much. One of the things I wanted to clarify is that, I think I understand what you're saying, but you advocate link level encryption instead of end to end. I believe, once I read your whole testimony, it occurred to me that what you're really talking about is an advocating of link level encryption, given that the message itself is signed and encrypted end to end, right?

Garry Binder – Intel – Senior Architect, Chronic Disease Management Group
You're exactly right. What we're advocating in terms of link level encryption just to take it one layer deeper is that this is probably the best, more accessible mechanism for protecting the confidentiality of a message. However, we do believe that there are cases that can be made for including an end-to-end encryption strategy in addition to whatever transport level or link level encryption is in place. It's not really an either/or, we're saying that we believe that link is a good base level position to take. If needed, there are the end-to-end technologies that can be used too.

Eric Dishman – Intel Digital Health Group – Director Health Innovation & Policy
We use that in our product today, the link level security.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I just didn't want to convey, didn't want anybody to think that link level is adequate in and of itself. If the message itself is not encrypted, so thank you.

Garry Binder – Intel – Senior Architect, Chronic Disease Management Group
Right, yes.

John Halamka – Harvard Medical School – Chief Information Officer
Any other comments or thoughts? Okay, well very good, thanks very much to Eric and Garry and Rick. Let me just summarize where I think in the six vendor testimony presentations, we've heard such things as directories could be as variables as a single centralized and managed directory for the country to no directory whatsoever. In the sense that e-mail has no directory, you have to know the e-mail address ahead of time, and then there was a routing mechanism that is organization to organization that gets delivery of the package.

That identity and trust is absolutely key in foundational. I think we've heard quite a lot of similarity in the testimony about how identity and trust is managed. Where there's a set of technologies, but importantly there's a set of management processes that ensure identity and create a trust fabric. That transport has been SMTP, S/MIME, REST, and SOAP, all implemented for various use cases successfully. I think we've heard quite a lot of good support, Arien, for SMTP and S/MIME, to the point of your achieving a consensus statement in your meetings. No one has objected to S/MIME and SMTP as a mechanism of getting a package from place to place in a simple and direct fashion.

I'll reflect for a moment on the Internet itself. The Internet itself has a reasonably small number of standards for directories, that is the DNS system. It has a reasonably small number of standards around certificate authorities, and using technology to create a trust fabric. But then there are multiple transport

standards that leverage the DNS and the certificate standards, which include everything that we've talked about today, HTP, FTP, SMTP, etc. So that generally, I think today's testimony has been quite consistent. I mean we've heard slight variations, but I think we've heard common themes about what is necessary and the spectrum of possibilities in the implementation of what is necessary.

Now more specifically, we as a committee have a next step, and that is to evaluate the direct project on its own merits. We've now heard this foundational testimony, and I think we're now empowered to take a look at the direct project and ask the question, is the implementation guidance provided by that project simple, direct, scalable, and secure to meet the goals that have been articulated by ONC and the project participants? That I certainly look forward to the activities that Dixie will lead in doing with her group that objective evaluation.

Now, I would welcome comments from Arien and Doug and others in the committee as to the gold star lessons you heard about today or any other comments you would have.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Well, I'm always available, John. I just wanted to make one tiny suggestion to your summary, which is not that e-mail doesn't have a directory, but that it has ad hoc directory solutions that are different for an enterprise and for a community and for the nation.

John Halamka – Harvard Medical School – Chief Information Officer
A very fair statement, and then the question of course is, is that directory local or is it discoverable by others outside of the organization? The answer is, of course, it does have a local directory. In fact, you may even have a local directory within your client. So yes, directories exist. It's probably a question of the scope of those directories and the discoverability.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes and the degree to which people want their address to be discoverable, but yes, right, exactly.

John Halamka – Harvard Medical School – Chief Information Officer
Very true.

Peter Tippett – Verizon Business – Vice President Research & Technology
John, we've gone back and forth a couple of times on the notion of encrypting the message for the tunnel or both. I did want to point out, the main thing I'm worried about, although the vast majority of messages are, certainly ought to be encrypted independent of how they're moved. The whole world is moving to a Cloud infrastructure. It is as big a revolution as the revolution between mainframes to PCs or between PCs and the Internet. If we insist on end-to-end encryption of the message, depending on what you call the end, we will make it impossible to use the Cloud infrastructure.

This is why I believe strongly that the last mile might need to be and is perfectly appropriate to be, the encryption only, where the end point can still be and the person using it can be well authenticated. Does that make sense? If we're going to, we have now probably every vendor on this call has cloud-based futures and current applications. People getting to them with some sort of a device that doesn't need to necessarily be smart, and as long as you can make sure that the end user is who they say they are, I can't imagine an increased and improved value of also keeping the message encrypted in addition to the pipe for that last bit.

Arien Malec – RelayHealth – VP, Product Management
That's exactly the place that we came to in the direct project, which is looking at end-to-end encryption between networks, but loss of flexibility for how those networks connect to the edges. John, I would endorse your summary, and say that we got to a place in the direct project where we concluded that the critical issues were issues scaling trust and scaling particularly federated trust across a pretty diverse set of healthcare settings. That you could skin the cat in terms of transport a bunch of different ways. In fact, we had four working implementations that were able to do the job.

We really came at a place where it was pick one, roll with it, and focus most of the attention on the policy and the technology platforms that allow us to scale trust across the nation. Then to the extent that there's a lot of energy and enthusiasm for transport standards that we actually probably should be directing a lot of our energy towards the common policy and trust fabric that allow us to scale trust nationwide.

John Halamka – Harvard Medical School – Chief Information Officer
Very well said. When I, some years ago, worked on some very, very basic, what I'll call secured e-mail technologies back in the day before it wasn't so easy. What we decided was trying to issue certificates and requiring S/MIME down to the level of the sender and recipient was actually not very scalable and not very supportable, but it was really straightforward to ensure network-to-network trust and organizational-to-organizational guaranteed delivery. I'm hearing these same tensions in your comments and Peter's comments.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I just want to make a couple comments. One, I am in violate agreement with Arien, in that and his testimony today even further reinforces it, that the essential thing is the trust fabric, not the method of the transport. I think from his testimony, I learned that that trust fabric needs to include both the common policies for issuing and managing the X509 certificates to people and software entities both, and common policies for managing the directory information as you've frequently pointed out.

I was surprised to learn, probably most surprised of anything today, that certificates are being issued to people, departments, and servers, and that people certificates are being used for SSL end point authentication. I think that that variety of use of certificates and variety of policies relating to the issuance and use of certificates is really an important value coming out of his testimony that certainly points to a need for a uniform policy there.

I also think that to take this opportunity to stress that we also need common policy relating mutual authentication, encryption, integrity protection, and non-repudiation of receipt. Even though everybody that gave testimony today, most people, everybody gave mutual authentication encryption, integrity protection, and most testifiers also gave non-repudiation of receipt. It's not really required; none of them are required by HIPAA today. I think that this is something that we need to stress that there needs to be policy in place that really ... that those be there.

It doesn't seem necessary at all that everyone use the same transport protocol. Although, it will be necessary for us to have a standard protocol for identifying and agreeing upon the transport to use between any two end points, because you can't have one side using REST and the other using SOAP or one side using SMTP and the other using SOAP.

The final thing I wanted to point out is that thanks to Intel's testimony, I'm reminded that that end point IP address may not be routable and that we do need to consider alternate protocols for that last leg of the exchange.

John Halamka – Harvard Medical School – Chief Information Officer
Great, as usual an elegant summary. Thank you. Other comments people have?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I have different hats to wear and I have to be careful which one I'm wearing. But if I wear the hat of the person who's been involved with the direct project, I think that you could make the case that what we've heard today kind of describes the scenario of not too different from the emergence of universal addressing as we know it today in e-mail.

Those of you, most of us unfortunately are probably old enough to remember the AOL copy serve local enterprise e-mail, UUCT soup of incompatible mail systems, not too many decades ago; which with the emergence of DNS and with the emergence of the definition of SMTP slowly gave way to true universal addressing. Where no matter who provided your last mile messaging capability, you could pipe in a well

formed address that didn't require lots of bang symbols and other crazy parenthetical expressions like the OUUCT model required, and be guaranteed that your message would find the recipient.

It seems to me that we're poised to see the same thing happen now with secure messaging in healthcare, where we've got a number of established players who are providing proprietary's secure messaging systems. What's missing is this way to bridge around universal addressing. Obviously, many other things downstream missing, such as the directory services and the like, but it will be very interesting to see if ontogeny recapitulates phylogeny in this space over the next few years. I think with my direct hat on, I believe that direct gives us an opportunity to do that. I guess I have to put my standards committee hat on and evaluate the … of that statement in the next phase.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
David, could you explain those three words?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Ontogeny recapitulates phylogeny?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes, those three.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's just the famous old rubric from arguments about whether the development of the embryo recapitulated the evolutionary heritage of human beings. Completely irrelevant, but just a fun thing to say.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
In other words, we have to go through the same steps.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, we go through the same process—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Right, yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
—that the evolution of the technologies went through.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Thanks. John, can I add a little bit, please?

John Halamka – Harvard Medical School – Chief Information Officer
Please do.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Okay, I think we always on these committees, and particularly with good testimony like today, we end up trying to maintain two balloons in our head. One balloon is the vision of the future and the other balloon is what can be done in the timeframes of the various deadlines for meaningful use.

I think it is good to know that there are individual people, certificates being issued, and that at the same time we want to recognize the accelerating nature of using certificates related to organizations and letting the organization be responsible for individuating the actual recipient, be it a department or a person based on internal rules. Both are important to keep in mind, neither one gives up the other.

Then on the issue that Peter raised with respect to being careful not to lose the value of the cloud, I think there's three levels of looking at that, and it's something that we've discussed quite a bit within other committees with respect to consent. One level is where it's a point-to-point transmission and the purpose

of the cloud is simply to enable that transition. The idea there would be that the cloud entity have no knowledge of the content. The compromise and the middle level, there's a need to decrypt and re-encrypt in order to match protocols, but there's no retention of information in the cloud.

The third level where somehow by virtual of having of retaining that information in the cloud as its passed through, there is value added, then really important issues of patient consent become invoked, much more challenging issues than those where the purpose is to get the information from point A to point B.

John Halamka – Harvard Medical School – Chief Information Officer
Very good. Any other comments from committee members?

Doug Fridsma – ONC – Acting Director, Office of Standards & Interoperability
I would just echo the comments that have been made so far. I think the one thing that I might add though is one of the themes that I see through this, and it's probably out of scope of this particular evaluation. But probably something that the HIT standards committee needs to put on their plate is that there appears to be the coming challenge of moving from exchange, which is just the moving of information back and forth, to this incrementalism towards interoperability that Wes has described.

I think I see that in a number of the different written testimonies and information that people have said in their presentations is that having multiple but limited and manageable number of transport options I think is going to be helpful. We've identified sort of a limited set that will work in different use cases, but there is going to be the coming challenge of semantics and interoperability. We need to figure out a strategy for how we get from the current notion of exchange, just making sure that we can move information around, to the point that we can actually begin to start using that in useful ways.

John Halamka – Harvard Medical School – Chief Information Officer
Correct.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Well, I have to say, one ... and two, a PDF is useful. I think that what we want is to establish a ladder or a stair step of levels of usefulness and move towards each level without denying the benefits of the lower level until we get to the higher level.

Doug Fridsma – ONC – Acting Director, Office of Standards & Interoperability
....

John Halamka – Harvard Medical School – Chief Information Officer
Boy, everybody is using such wonderful aphorisms today.

Doug Fridsma – ONC – Acting Director, Office of Standards & Interoperability
Maybe our next meeting will be in Latin.

John Halamka – Harvard Medical School – Chief Information Officer
Okay.

James Walker – Geisinger Health System – CHIO
For the future, I have a suspicion that the complexity of information sharing, shared development, and sharing the information itself, really will be almost qualitatively more complex as we try to support ACO like things.

John Halamka – Harvard Medical School – Chief Information Officer
Right and I recognize that in ACO Nirvana, everyone will share every bit of information for care coordination, population health, quality and an efficiency, and boy, is it going to get more complicated.

James Walker – Geisinger Health System – CHIO

I think what we will do is not share everything, but what will be required for ACOs not to drown, for there to be clear. That's probably beyond HIT standards, agreements about what is worth collecting and in what ways and for whom and by whom and a whole set of realities that currently we cannot pay attention to and get away with it.

John Halamka – Harvard Medical School – Chief Information Officer
Correct.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes, ACO Nirvana is everybody getting exactly the information they need, not all information and never missing any information they need.

James Walker – Geisinger Health System – CHIO
Right.

John Halamka – Harvard Medical School – Chief Information Officer
That is very true.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
And it goes way beyond direct simple push messaging.

John Halamka – Harvard Medical School – Chief Information Officer
That is right.

James Walker – Geisinger Health System – CHIO
Absolutely.

John Halamka – Harvard Medical School – Chief Information Officer
Well, great, a very, very rich discussion today. As I said, next steps are based on all of this foundation we have heard about today. We will commence an evaluation of the direct project on its own merits, evaluating its specific goals about being simple and secure and direct and scalable. Then of course, share all of that with the broader committee and give the feedback to Arien and to Doug and to your groups that you have asked us to do in this formal evaluation.

James Walker – Geisinger Health System – CHIO
John, just real quickly, I just want to thank all of the presenters. This was just an exemplary set of very useful presentations.

John Halamka – Harvard Medical School – Chief Information Officer
Yes, I agree. I come away with hope that yes, convergence and consensus is possible, that we today heard that there is actually a finite number of solutions to the push problem, and we've heard what's the priority to solve and where we can allow variability. So I agree, a very, very rich day. Thanks so much to everyone.

Jon Perlin, let me turn it back to you, any closing comments you would make, and then I know we have our public comment.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Well, just thank you, John. I would just echo the appreciation to all the presenters and all participants and a very rich discussion. It really reinforces the optimism of the world ahead. I think Wes' metaphor of the two balloons, not only the nirvana of what we get to, but really the capacity to use some of these technologies in the near term.

John, before we go onto public comment, let me just ask Doug Fridsma if he wants to add anything additionally on next steps more broadly or save that for next meeting.

Doug Fridsma – ONC – Acting Director, Office of Standards & Interoperability
No, I think there are probably some other things that we need to get on the agenda to talk about. I think that there's been a really nice summary of the activities that we need to take a look at. I think John did a really nice job of summarizing those activities. We'll need to take those, take a look at what that means in terms of the work that is ahead of us here at ONC.

Then probably come back to the committee at some point and say given the recommendations and the testimony that we received today—as well as some of the other standards and work that has been adopted over the course of the last couple of months just as you are going to be looking ahead to stage two and stage three meaningful use—we also need to think about what is the work ahead for us. How do we establish those priorities and the like? I think we probably don't have time to talk about that today, but I think we'll take all of this information in the discussion and hopefully be able to at the next meeting present some of the things that we may need to be doing over the course of the next couple of weeks to a month.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Terrific, so we'll look forward to that in the days, and I think that's some future agenda activity. Just a reminder, I believe our next meeting is December 17th, Judy?

Judy Sparrow – Office of the National Coordinator – Executive Director
Yes, that's correct, December 17th, and again, a virtual meeting.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Okay. My thanks to all of the ONC staff, all of the participants, all of the presenters today. Let's move to the public comment period, and Judy, I will turn it back to you to see if there are any calls or Web inquiries.

Judy Sparrow – Office of the National Coordinator – Executive Director
Great, thank you. We would like to invite public comment at this time. Let's just wait a moment to see if anybody dials in.

John Halamka – Harvard Medical School – Chief Information Officer
Well, we've had such a rich discussion today, one other thing I should mention, I supposed that the HIE Workgroup of the HIT Policy Committee is working on a set of policies around provider directories. Claudia, if you're still on the line, I presume at some point we're going to get a handoff from the policy committee to the standards committee with that input and guidance as we start thinking about the standards for provider directories and addressing.

Judy Sparrow – Office of the National Coordinator – Executive Director
John, actually I'm going to be sending you a transmittal letter on the outcome of the policy committee last week or whenever that was on the Information Exchange Workgroup.

John Halamka – Harvard Medical School – Chief Information Officer
Great. Arien and I would presume that the addressing schemas that you have worked out thus far in the directory thinking is probably very well-aligned with the HIE Workgroup's efforts in this regard. So Judy, if there's anything you can handoff to us, that would just simply help us in our evaluation.

Judy Sparrow – Office of the National Coordinator – Executive Director
That's right. I'll be sending that later today. It doesn't sound like we have any public comment.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Okay, well again, thanks to all participants, especially the presenters, ONC staff, and committee members, John Halamka, thank you very much. We'll look forward to reconvening on Friday, December 17th. Thanks again.

Judy Sparrow – Office of the National Coordinator – Executive Director

Thanks so much.

John Halamka – Harvard Medical School – Chief Information Officer
Have a great holiday, thanks so much everybody.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Goodbye.

Judy Sparrow – Office of the National Coordinator – Executive Director
Goodbye.

Jonathan Perlin – Hospital Corporation of America – CMO & President
Goodbye.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Goodbye.

Public Comment Received During the Meeting

1. If an end-user is using Surescripts through an EHR, can provider send patient encounter data to other entities involved in their healthcare? How will this work exactly? Such as will Surescripts transport the data to the State's HIE which will connect to NHIN... Thanks!

2. How does this reflect EHR preference for SOAP-based transactions?